PATENT ABSTRACTS OF JAPAN

(11) Publication number : 11-346210
(43) Date of publication of application : 14.12.1999

(51) Int.Cl. H04L 9/08
G09C 1/00
H04L 9/32

(21) Application number : 10-152866
(22) Date of filing : 02.06.1998

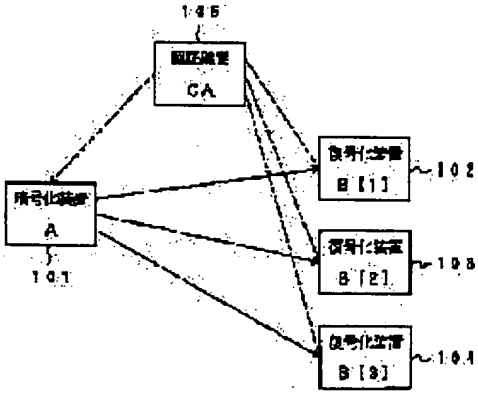
(71) Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72) Inventor : ARAKAWA MEGUMI
WATABE KATSUTOSHI
TAMANO DAISUKE

(54) ENCRYPTION METHOD AND DEVICE, DECODING METHOD AND DEVICE, RECORD MEDIUM RECORDING ENCRYPTION PROGRAM, RECORD MEDIUM RECORDING DECODING PROGRAM, METHOD FOR ELECTRONIC SIGNATURE AND METHOD FOR AUTHENTICATING ELECTRONIC SIGNATURE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide the encryption method and device and the decoding method and device by which a group encryption for a public key system is realized while keeping a form of one privacy key possessed by one person and one public key open to a certificate agency (CA) so as to attain secure and simple key delivery and to simply generate an optional group, and to provide the record medium recording an encryption program and the record medium recording a decoding program.

SOLUTION: The encryption method that is used when a file sender distributes files to one or plural recipients includes at least a step where the sender encrypts the files by using a symmetric key, a step where the sender encrypts the symmetric key by using a private key of the sender and a public key of the recipients, and a step where the sender sends the encrypted files and the encrypted symmetric key.



LEGAL STATUS

[Date of request for examination] 14.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－346210

(43)公開日　平成11年(1999)12月14日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６０１Ｅ
			６７５Ｄ

審査請求　未請求　請求項の数36　ＯＬ　（全 25 頁）

(21)出願番号　特願平10－152866

(22)出願日　平成10年(1998)６月２日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号

(72)発明者　荒川　恵
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　渡部　勝年
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　玉野　大祐
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

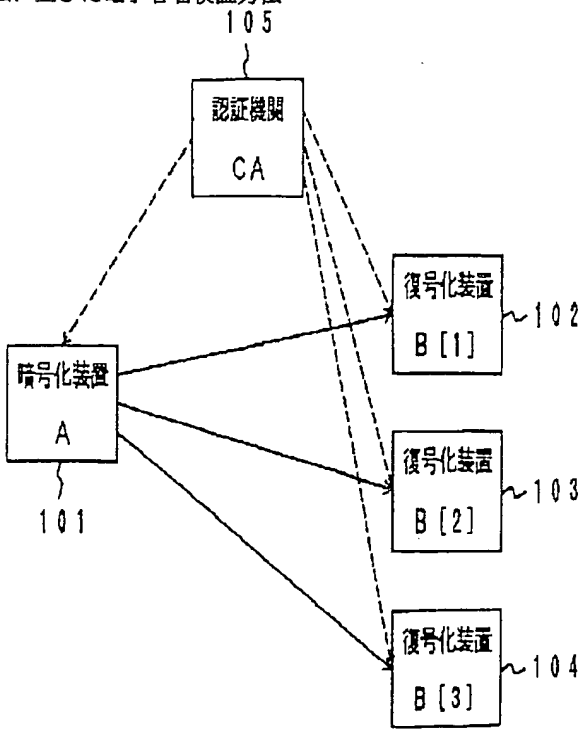
(74)代理人　弁理士　鈴江　武彦　（外２名）

(54)【発明の名称】暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、復号化プログラムを記録した記録媒体、電子署名方法、並びに電子署名検証方法

(57)【要約】

【課題】本発明の課題は、個人が持つ１つの秘密鍵、認証機関（ＣＡ）に公開されている１つの公開鍵という形態のままで公開鍵方式のグループ暗号を実現することにより、鍵配送が安全でかつ簡単であり、さらに任意のグループを簡単に作成する事ができる暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、並びに復号化プログラムを記録した記録媒体を提供することにある。

【解決手段】本発明は、ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を送信するステップとを少なくとも持つことを特徴とする暗号化方法。



【特許請求の範囲】

【請求項１】　ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、
対称鍵を用いて該ファイルを暗号化するステップと、
該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、
前記暗号化したファイルと前記暗号化した対称鍵を送信するステップとを少なくとも持つことを特徴とする暗号化方法。

【請求項２】　ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、
対称鍵を用いて該ファイルを暗号化するステップと、
該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、
前記暗号化したファイルと前記暗号化した対称鍵を記録媒体に記録して受信者へ渡すステップとを少なくとも持つことを特徴とする暗号化方法。

【請求項３】　前記ファイルに関する情報を対称鍵を用いて暗号化するステップを持つことを特徴とする請求項１又は２記載の暗号化方法。

【請求項４】　前記ファイル内容及びファイルに関する情報に電子署名情報を付与することを特徴とする請求項３記載の暗号化方法。

【請求項５】　少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする請求項１、２、３又は４記載の暗号化方法。

【請求項６】　暗号化されたファイル及び対称鍵を復号化する復号化方法であって、
前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、
該復号化された対称鍵を用いて前記暗号化されたファイルを復号化するステップとを少なくとも持つことを特徴とする復号化方法。

【請求項７】　暗号化されたファイル及び対称鍵を復号化する復号化方法であって、
前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、
該復号化された対称鍵を用いて前記暗号化されたファイルを復号化するステップと、
復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定するステップを持つことを特徴とする復号化方法。

【請求項８】　少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする請求項６又は７記載の復号化方法。

【請求項９】　対称鍵を発生する対称鍵発生手段と、
この対称鍵発生手段で発生した対称鍵でファイルを暗号化するファイル暗号化手段と、
前記対称鍵発生手段で発生した対称鍵を送信者の秘密鍵と受信者の公開鍵で暗号化する対称鍵暗号化手段と、
この対称鍵暗号化手段で暗号化した対称鍵と前記ファイル暗号化手段で暗号化したファイルを連結する連結手段とを具備することを特徴とする暗号化装置。

【請求項１０】　対称鍵を発生する対称鍵発生手段と、
この対称鍵発生手段で発生した対称鍵でファイルを暗号化するファイル暗号化手段と、
前記対称鍵発生手段で発生した対称鍵でファイルに関する情報を暗号化するファイル情報暗号化手段と、
前記対称鍵発生手段で発生した対称鍵を送信者の秘密鍵と受信者の公開鍵で暗号化する対称鍵暗号化手段と、
この対称鍵暗号化手段で暗号化した対称鍵と前記ファイル暗号化手段で暗号化したファイルと前記ファイル情報暗号化手段で暗号化したファイルに関する情報を連結する連結手段とを具備することを特徴とする暗号化装置。

【請求項１１】　ファイル内容及びファイルに関する情報に送信者の署名用秘密鍵で電子署名情報を付与する電子署名手段を具備することを特徴とする請求項９又は１０記載の暗号化装置。

【請求項１２】　暗号データから暗号化された対称鍵と暗号化されたファイルを分離する暗号データ分離手段と、
この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、
この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイルを復号化するファイル復号化手段とを具備することを特徴とする復号化装置。

【請求項１３】　暗号データから暗号化された対称鍵と暗号化された電子署名付ファイルを分離する暗号データ分離手段と、
この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、
この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルを復号化するファイル復号化手段と、
このファイル復号化手段で復号化された電子署名付ファイルを送信者の署名用公開鍵を用いて電子署名を分離して検証する電子署名分離・検証手段とを具備することを特徴とする復号化装置。

【請求項１４】　暗号データから暗号化された対称鍵と暗号化されたファイルに関する情報と暗号化されたファイル内容を分離する暗号データ分離手段と、
この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、

この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイル情報を復号化するファイル情報復号化手段と、
前記対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイルを復号化するファイル復号化手段とを具備することを特徴とする復号化装置。
【請求項１５】　暗号データから暗号化された対称鍵と暗号化された電子署名付ファイルに関する情報と暗号化された電子署名付ファイルを分離する暗号データ分離手段と、
この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、
この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルに関する情報を復号化するファイルに関する情報復号化手段と、
前記対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルを復号化するファイル復号化手段と、
このファイル復号化手段で復号化された電子署名付ファイルと前記ファイル情報復号化手段で復号化された電子署名付ファイル情報を送信者の署名用公開鍵を用いて電子署名を分離して検証する電子署名分離・検証手段とを具備することを特徴とする復号化装置。
【請求項１６】　復号化されたファイル情報に基づいて所定のファイルを選択して復号化するファイル選択手段を具備することを特徴とする請求項１４又は１５記載の復号化装置。
【請求項１７】　ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化プログラムを記録した記録媒体であって、
対称鍵を用いて該ファイルを暗号化する手順、
該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化する手順、
前記暗号化したファイルと前記暗号化した対称鍵を送信する手順を実行させるための暗号化プログラムを記録した記録媒体。
【請求項１８】　前記ファイルに関する情報を対称鍵を用いて暗号化する手順を実行させるためのプログラムを記録したことを特徴とする請求項１７記載の暗号化プログラムを記録した記録媒体。
【請求項１９】　前記ファイル及びファイルに関する情報に電子署名情報を付与するためのプログラムを記録したことを特徴とする請求項１８記載の暗号化プログラムを記録した記録媒体。
【請求項２０】　少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するためのプログラムを記録したことを特徴とする請求項１７、１８又は１９記載の暗号化プログラムを記録した記録媒体。
【請求項２１】　暗号化されたファイル内容又はファイルに関する情報及び対称鍵を復号化するためのプログラムを記録した記録媒体であって、
前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化する手順、
該復号化された対称鍵を用いて前記暗号化されたファイル内容又はファイルに関する情報を復号化する手順を実行させるための復号化プログラムを記録した記録媒体。
【請求項２２】　前記復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定する手順を実行させるためのプログラムを記録したことを特徴とする請求項２１記載の復号化プログラムを記録した記録媒体。
【請求項２３】　少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するためのプログラムを記録したことを特徴とする請求項２１又は２２記載の復号化プログラムを記録した記録媒体。
【請求項２４】　ファイルの所有者が複数の閲覧者（所有者を含む）へ該ファイルを暗号化する方法であって、
対称鍵を用いて前記ファイルを暗号化するステップと、
該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、
前記暗号化したファイルと該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。
【請求項２５】　ファイルの所有者が複数の閲覧者（所有者を含む）へファイルの内容と該ファイルに関する情報を暗号化する方法であって、
該ファイルを該ファイル内容と該ファイルに関する情報に分離するステップと、
対称鍵を用いて前記ファイル内容と前記ファイルに関する情報を暗号化するステップと、
該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、
前記暗号化したファイル内容と前記暗号化したファイルに関する情報と該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。
【請求項２６】　ファイルの所有者が複数の閲覧者（所有者を含む）へ該ファイルを暗号化する方法であって、
前記所有者が前記閲覧者の情報を任意のグループに分けて管理するステップと、
該グループから、前記グループに属する閲覧者の情報を抽出するステップと、
前記閲覧者の情報から前記閲覧者の公開鍵をを抽出する

ステップと、
対称鍵を用いて前記ファイルを暗号化するステップと、
該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、
前記暗号化したファイルと該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。
【請求項２７】　ファイルの所有者が複数の閲覧者（所有者を含む）へファイル内容と該ファイルに関する情報を暗号化する方法であって、
前記所有者が前記閲覧者の情報を任意のグループに分けて管理するステップと、
該グループから、前記グループに属する閲覧者の情報を抽出するステップと、
前記閲覧者の情報から前記閲覧者の公開鍵をを抽出するステップと、
該ファイルを該ファイル内容と該ファイルに関する情報に分離するステップと、
対称鍵を用いて前記ファイル内容と前記ファイルに関する情報を暗号化するステップと、
該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、
前記暗号化したファイル内容と前記暗号化したファイルに関する情報と該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。
【請求項２８】　暗号化したファイルと暗号化済対称鍵全てを結合したものを復号化する方法であって、
前記暗号化したファイルと暗号化済対称鍵全てを結合したものから、前記暗号化したファイルと暗号化済対称鍵全てを分離するステップと、
所有者の公開鍵と閲覧者の秘密鍵を用いて前記暗号化済対称鍵を復号化するステップと、
該復号化された対称鍵を用いて該暗号化したファイルを復号化するステップとを少なくとも持つことを特徴とする復号化方法。
【請求項２９】　暗号化したファイル内容と暗号化したファイルに関する情報と暗号化済対称鍵全てを結合したものを復号化する方法であって、
前記暗号化したファイル内容と前記暗号化したファイルに関する情報と暗号化済対称鍵全てを結合したものから、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と暗号化済対称鍵全てを分離するステップと、
所有者の公開鍵と閲覧者の秘密鍵を用いて前記暗号化済対称鍵を復号化するステップと、
該復号化された対称鍵を用いて該暗号化したファイル内容と該暗号化したファイルに関する情報を復号化するステップと、
該復号化されたファイル内容と該復号化されたファイルに関する情報を結合し前記ファイルを再構成するステップとを少なくとも持つことを特徴とする復号化方法。
【請求項３０】　復号化されたファイルに関する情報に基き、閲覧者側で復号化すべきファイルを指定するステップと、
復号化された対称鍵を用いて暗号化したファイルのうち指定された該復号化すべきファイルを復号化するステップとを持つことを特徴とする復号化方法。
【請求項３１】　所有者の秘密鍵を用いて前記ファイルの電子署名を生成するステップと、
前記ファイルに該電子署名を結合するステップとを持つことを特徴とする電子署名方法。
【請求項３２】　所有者の秘密鍵を用いて前記ファイル内容の電子署名を生成するステップと、
前記ファイル内容に該電子署名を結合するステップとを持つことを特徴とする電子署名方法。
【請求項３３】　所有者の秘密鍵を用いて前記ファイルに関する情報の電子署名を生成するステップと、
前記ファイルに関する情報に該電子署名を結合するステップとを持つことを特徴とする電子署名方法。
【請求項３４】　ファイルから電子署名を分離するステップと、
所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。
【請求項３５】　ファイル内容から電子署名を分離するステップと、
所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。
【請求項３６】　ファイルに関する情報から電子署名を分離するステップと、
所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はファイルの送信者が１人又は複数の受信者へ該ファイルを秘密に配布するための暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、復号化プログラムを記録した記録媒体、電子署名方法、並びに電子署名検証方法に関する。
【０００２】
【従来の技術】今日、ＯＡ化等により、文書等の電子化が進んでいる。これに伴い重要な電子情報が増えてきており、第三者の不正（盗み見、改ざん、なりすまし）から、守る必要が出てきた。
【０００３】上記要望を満たすべく、ファイルに暗号および電子署名処理を施し上記の脅威から守る、ファイル暗号ソフトウェアが現れた。当初、ファイル暗号ソフトウェアは、個人のファイルを守ることをメインに考えら

れていたが、情報化が進み各企業でイントラネット等のネットワーク構築が行われる中、ファイルサーバ上で暗号化されたファイルを共有的に利用するため、ある指定されたグループの人しか見る事ができないというような、グループ暗号の必要性が出てきた。

【０００４】グループでのファイル共有を実現するため、現状では以下の方式が用いられている。

（１）　復号時に必要なパスワードをグループで共有するパスワード方式。

【０００５】すなわち、送信者はパスワードを用いて暗号ファイルを作成し、当該パスワードをグループの受信者に通知する。グループの受信者は当該パスワードを用いて送信者から送信された暗号ファイルを復号化する。グループ以外の受信者は当該パスワードがないため送信者から送信された暗号ファイルを復号化することができない。

【０００６】（２）　復号時に必要なグループ鍵をグループで共有するグループ鍵共有方式。すなわち、送信者はグループ鍵を用いて暗号ファイルを作成し、当該グループ鍵をグループの受信者に通知する。グループの受信者は当該グループ鍵を用いて送信者から送信された暗号ファイルを復号化する。グループ以外の受信者は当該グループ鍵がないため送信者から送信された暗号ファイルを復号化することができない。

【０００７】

【発明が解決しようとする課題】パスワード方式では以下のような欠点がある。

（１）　グループ全員に暗号ファイルを作成するたびにパスワードを第三者に秘密に配送しなければならない。

【０００８】（２）　各暗号ファイル（グループ）ごとにパスワードが増えるので管理が非常に大変である。

（３）　どのパスワードがどの暗号ファイルのものか分からなくなる。

【０００９】（４）　パスワードを忘れてしまう。

また、グループ鍵共有方式では以下のような欠点がある。

（１）　暗号ファイル毎にグループの構成が異なる場合には、グループを構成するたびにグループ鍵を第三者に秘密にグループ全員に配送しなければならない。

【００１０】（２）　グループを構成するごとにグループ鍵が増えるので管理が非常に大変である。

（３）　どのグループ鍵がどのグループのものか分からなくなる。

【００１１】（４）　グループ鍵を忘れてしまう。

本発明は上記の事情に鑑みてなされたもので、個人が持つ１つの秘密鍵、認証機関（ＣＡ）に公開されている１つの公開鍵という形態のままで公開鍵方式のグループ暗号を実現することにより、鍵配送が安全でかつ簡単であり、さらに任意のグループを簡単に作成する事ができる暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、復号化プログラムを記録した記録媒体、電子署名方法、並びに電子署名検証方法を提供することを目的とする。

【００１２】

【課題を解決するための手段】上記目的を達成するために本発明は、ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を送信するステップとを少なくとも持つことを特徴とする。

【００１３】また本発明は、ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を記録媒体に記録して受信者へ渡すステップとを少なくとも持つことを特徴とする暗号化方法。

【００１４】また本発明は、前記ファイルに関する情報を対称鍵を用いて暗号化するステップを持つことを特徴とする。また本発明は、前記ファイル及びファイルに関する情報に電子署名情報を付与することを特徴とする。

【００１５】.また本発明は、少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする。また本発明は、暗号化されたファイル又はファイルに関する情報及び対称鍵を復号化する復号化方法であって、前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、該復号化された対称鍵を用いて前記暗号化されたファイル又はファイルに関する情報を復号化するステップとを少なくとも持つことを特徴とする。

【００１６】また本発明は、前記復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定するステップを持つことを特徴とする。また本発明は、少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする。

【００１７】

【発明の実施の形態】以下図面を参照して本発明の実施の形態例を詳細に説明する。先ず、本発明の実施形態例に表記される記号について説明する。

『公開鍵暗号方式の鍵の表記』

（１）　先頭２文字

ＰＫ：公開鍵

ＳＫ：秘密鍵

（２）　次の１文字

ｄ：鍵配送に使用する鍵

ｓ：電子署名に使用する鍵
（３）　４文字目以降
鍵を所持している装置名
（４）　例
ＰＫｄＡ＝装置Ａの鍵配送用（ｄ）の公開鍵（ＰＫ）
（５）　本発明で使用される鍵
・暗号化装置Ａの鍵
ＰＫｄＡ　　Ａの鍵配送用鍵の公開鍵
ＳＫｄＡ　　Ａの鍵配送用鍵の秘密鍵
ＰＫｓＡ　　Ａの電子署名用鍵の公開鍵
ＳＫｓＡ　　Ａの電子署名用鍵の秘密鍵
・復号化装置Ｂの鍵
ＰＫｄＢ　　Ｂの鍵配送用鍵の公開鍵
ＳＫｄＢ　　Ｂの鍵配送用鍵の秘密鍵
ＰＫｓＢ　　Ｂの電子署名用鍵の公開鍵
ＳＫｓＢ　　Ｂの電子署名用鍵の秘密鍵
『関数などの表記』
Ｃｅｒｔ（）：証明書
（例）　Ｃｅｒｔ（ＰＫｄＡ）＝ＰＫｄＡの証明書
ｈ（）：ハッシュ関数
（例）　ｈ（Ｍ）：平文Ｍのハッシュダイジェスト
「電子署名の生成」
（例）　ＳＫｓＡ（ｈ（Ｍ））：平文Ｍに対するＡの電子署名
平文Ｍのハッシュダイジェストを署名用秘密鍵ＳＫｓＡで暗号化したもの。
【００１８】通常は平文Ｍに添付し、Ｍ‖ＳＫｓＡ（ｈ（Ｍ））とする。
「電子署名の検証」
（例）　復号装置が、Ａの電子署名付き平文Ｍ‖ＳＫｓＡ（ｈ（Ｍ））を受け取ったとき、
（１）　Ｍ→ｈ（Ｍ）：ハッシュ関数を使用
（２）　ＳＫｓＡ（ｈ（Ｍ））→ｈ（Ｍ）：電子署名の復号化
（３）　（１）と（２）を比較することが検証に該当し、一致していればＯＫであり、一致しなければＮＧである。
【００１９】‖：連結
ＤＥＫ：セッションキー（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ）であり、平文の暗号化を行う対称鍵方式の対称鍵である。ランダム生成で、通信ごとに使い捨てである。
【００２０】Ｋｅｙ（Ｍ）：暗号化。「鍵名（暗号化対象）」と書く
［］：配列
…：中略
（例）　Ｂ［ｉ］（ｉ＝１、…、ｎ）：同様の機能を有するｎ個の装置
（例）　Ｍ［ｊ］（ｊ＝１、…、ｔ）：ｔ個の平文Ｍ
（例）　ＰＫｄＢ［１］（ＤＥＫ）‖…‖ＰＫｄＢ［ｎ］（ＤＥＫ）：暗号化して連結したｎ個のデータ
『公開鍵方式について』
「公開鍵には大きく分けて以下の２種類がある。」
（１）　ＲＳＡ等の通常の公開鍵方式
暗号化装置Ｘ、復号化装置Ｙとする。
【００２１】暗号化装置Ｘから復号化装置ＹへＤＥＫを安全に送信するときの方法は以下のようになる。暗号化装置Ｘは、ＤＥＫを公開鍵ＰＫｄＹで暗号化し、ＰＫｄＹ（ＤＥＫ）となる。一方復号化装置Ｙは、ＰＫｄＹ（ＤＥＫ）を秘密鍵ＳＫｄＹで復号化し、ＤＥＫを得る。
【００２２】（２）　ＤＨ・楕円ＤＨ等の共有鍵を用いた公開鍵方式
暗号化装置Ｘ、復号化装置Ｙとする。暗号化装置Ｘから復号化装置ＹへＤＥＫを安全に送信するときの方法は以下のようになる。
【００２３】暗号化装置Ｘは、暗号化装置Ｘの秘密鍵ＳＫｄＸと復号化装置Ｙの公開鍵ＰＫｄＹから共有鍵ＳＸＹを生成する。ＤＥＫをＳＸＹで暗号化し、ＳＸＹ（ＤＥＫ）となる。
【００２４】一方、復号化装置Ｙは、暗号化装置Ｘの公開鍵ＰＫｄＸと復号化装置Ｙの秘密鍵ＳＫｄＹから共有鍵ＳＹＸを生成するが、ＤＨ・楕円ＤＨ等ではＳＹＸ＝ＳＸＹとなるように秘密鍵と公開鍵が作成されている。
【００２５】それゆえ、ＳＹＸ（＝ＳＸＹ）を生成し、ＳＸＹ（ＤＥＫ）を復号化し、ＤＥＫを得る。
（３）　ＤＨの詳細について
ａ、ｐを公開しているとする。ａは自然数、ｐは素数である。
【００２６】このとき暗号化装置Ｘの秘密鍵ＳＫｄＸと公開鍵ＰＫｄＸには以下のような関係がある。
ＰＫｄＸ＝ａ^{SKdX} ｍｏｄ　ｐ
ここで、ｍｏｄは剰余演算である。
【００２７】同様に、復号化装置Ｙの秘密鍵ＳＫｄＹと公開鍵ＰＫｄＹについても、
ＰＫｄＹ＝ａ^{SKdY} ｍｏｄ　ｐ
したがって、
ＳＸＹ＝ＰＫｄＹ^{SKdX} ｍｏｄ　ｐ
＝（ａ^{SKdY} ｍｏｄ　ｐ）^{SKdX} ｍｏｄ　ｐ
＝ａ$^{(SKdY*SKdX)}$ｍｏｄ　ｐ
ＳＹＸ＝ＰＫｄＸ^{SKdY} ｍｏｄ　ｐ
＝（ａ^{SKdX} ｍｏｄ　ｐ）^{SKdY} ｍｏｄ　ｐ
＝ａ$^{(SKdX*SKdY)}$ ｍｏｄ　ｐ
＝ａ$^{(SKdY*SKdX)}$ ｍｏｄ　ｐ＝ＳＸＹ
故にＳＸＹ＝ＳＹＸである。
【００２８】それゆえ暗号化装置Ｘと復号化装置Ｙは同じ共有鍵ＳＸＹを公開鍵の交換だけで生成できる。
「公開鍵を用いて暗号化を行うときの表記について」上記のように、公開鍵には
（１）　ＲＳＡ等の通常の公開鍵方式

（2）　DH・楕円DH等の共有鍵を用いた公開鍵方式の2種類があり、暗号化の方式が異なる。

【0029】これらの方式の鍵は、方法は異なるが同じ目的（DEKの暗号化・復号化）に用いられる。これらの鍵を同じように扱うため、

DEKの暗号化に用いる鍵を、Enc-X-Y

DEKの復号化に用いる鍵を、Dec-X-Y

と定義する。

・先頭3文字：鍵の種類

Enc：暗号化に使用される鍵

Dec：復号化に使用される鍵

・4文字目は「-」

・5文字目から「-」まで：暗号装置名

・次の「-」から末尾まで：復号装置名

例として、暗号装置Xと復号装置Yの間の鍵について記す。

【0030】（1）　では、

EncXY＝PKdY

DecXY＝SKdY

となり、暗号化装置Xには存在しない鍵となる。

【0031】（2）　では、

EncXY＝SKdXとPKdYから生成される鍵

DecXY＝PKdXとSKdYから生成される鍵

生成元は異なるが、EncXY＝DecXYである。

【0032】なお、本発明においては、公開鍵方式として2つの方式を想定しているが、これに限定される必要はなく、他の公開鍵方式でも可能である。また同様に、対称鍵方式についても他の対称鍵方式（共通鍵方式、秘密鍵方式）であってもよい。

【0033】次に、本発明の一実施形態例について説明する。図1は本発明の一実施形態例を示す構成説明図である。図において、101は送信者の暗号化装置Aであり、ファイルを暗号化する。102は受信者の復号化装置B［1］であり、暗号化されたファイルを復号化する。103は受信者の復号化装置B［2］であり、暗号化されたファイルを復号化する。104は受信者の復号化装置B［3］であり、暗号化されたファイルを復号化する。105は認証機関CAであり、暗号化装置A、復号化装置B［1］、復号化装置B［2］、復号化装置B［3］に公開鍵を提供する。

【0034】図2は図1の認証機関CAを介する場合の各装置間の動作フロー図であり、図3は図1の認証機関CAを介さない場合の各装置間の動作フロー図である。すなわち、図2に示すように、ステップ（Step）1において、暗号化装置Aは暗号化装置Aの鍵配送用鍵の公開鍵PKdA、暗号化装置Aの鍵配送用鍵の秘密鍵SKdA、暗号化装置Aの電子署名用鍵の公開鍵PKsA及び暗号化装置Aの電子署名用鍵の秘密鍵SKsAを生成し、このうち公開鍵PKdA及び公開鍵PKsAを認証機関CAに登録する。ステップ2において、認証機関CAは認証機関CAの証明書を登録する。ステップ3において、復号化装置B［i］（i＝1、…、n）は復号化装置B［i］の鍵配送用鍵の公開鍵PKdB［i］及び復号化装置B［i］の電子署名用鍵の公開鍵PKsB［i］を生成し、認証機関CAに登録する。ステップ4において、グループ暗号化を行う前に、暗号化装置Aは認証機関CAに公開鍵PKdB［i］を要求する。ステップ5において、認証機関CAは認証機関CAの証明書を配布する。ステップ6において、認証機関CAは暗号化装置Aに公開鍵PKdB［i］の証明書Cert（PKdB［i］）を暗号化装置Aに配布する。ステップ7において、後述する複数人暗号化を行う。ステップ8において、暗号化装置Aは暗号文Cを復号化装置B［i］に配布する。ステップ9において、復号化装置B［i］が暗号文Cを取得・復号化する前に、復号化装置B［i］は公開鍵PKdA及び公開鍵PKsAを認証機関CAに要求する。ステップ10において、認証機関CAは認証機関CAの証明書を配布する。ステップ11において、認証機関CAは公開鍵PKdAの証明書Cert（PKdA）及び公開鍵PKsAの証明書Cert（PKsA）を復号化装置B［i］に配布する。ステップ12において、後述する複数人復号化を行う。

【0035】また、図3の場合は、ステップ4において、グループ暗号化を行う前に、暗号化装置Aは復号化装置B［i］に必要に応じて公開鍵PKdB［i］を要求する。ステップ6において、暗号化装置Aは復号化装置B［i］から公開鍵PKdB［i］を取得する。ステップ7において、後述する複数人暗号化を行う。ステップ8において、暗号化装置Aは暗号文Cを復号化装置B［i］に配布する。ステップ9において、復号化装置B［i］が暗号文Cを取得・復号化する前に、復号化装置B［i］は必要に応じて公開鍵PKdA及び公開鍵PKsAを暗号化装置Aに要求する。ステップ11において、復号化装置B［i］は公開鍵PKdA及び公開鍵PKsAを暗号化装置Aから取得する。ステップ12において、後述する複数人復号化を行う。

【0036】図4は図2のステップ7に対応した暗号化装置Aの一例を示す構成説明図である。図4の各部を説明する。

（1）　ファイル情報分離器601

入力：暗号化するt個のファイルF［j］（j＝1、…、t）

出力：ファイル情報M［0］、ファイル内容M［j］（j＝1、…、t）

ファイルをそれぞれファイル情報（ファイル名、ファイルサイズ、日付、ディレクトリ構造の情報等）とファイル内容（ファイル情報を取り出したファイル中身）に分け、t個のファイル情報をひとつにまとめてM［0］とし、ファイル内容をM［1］、…、M［t］（ファイル中身F［1］、…、F［t］に対応）とする。

【００３７】（２）　グループ情報変換器６０２、グループ情報ＤＢ（データベース）６０３
入力：暗号化装置利用者名Ａまたは復号化装置利用グループ名Ｇ（復号装置Ｂ［ｉ］（ｉ＝１、…、ｎ））
出力：装置名（１以上）Ａ及びＢ［ｉ］（ｉ＝１、…、ｎ）
グループ情報ＤＢ６０３には、利用グループ名（利用者名）と装置名との対応関係が格納されている。このグループ情報ＤＢ６０３の情報を利用して、利用グループ名→利用者名→装置名と変換する。
【００３８】（３）　鍵検索器６０４、鍵ＤＢ６０５
入力：装置名Ａ及びＢ［ｉ］（ｉ＝１、…、ｎ）、要求元（鍵の要求元の情報。複数人暗号器または電子署名生成・連結器の情報）
出力：公開鍵方式の鍵。Ａの署名用秘密鍵ＳＫｓＡ、暗号化鍵Ｅｎｃ-Ａ-Ｂ［ｉ］（ｉ＝１、…、ｎ）
鍵ＤＢ６０５には、装置名とその公開鍵が格納されている。入力を基に、鍵ＤＢ６０５から秘密鍵・公開鍵を取り出して、暗号化鍵を生成し、要求元（複数人暗号器６０９や電子署名生成・連結器６０６）へ渡す。本発明ではＤＨの例を説明する（ＤＨでは暗号化装置の秘密鍵と復号化装置の公開鍵によって暗号化鍵を生成するが、ＲＳＡ等の公開鍵方式を用いて暗号化鍵を生成する場合は、復号化装置の公開鍵を暗号化鍵として用いる）。
【００３９】以降現れる単独のｊは、０≦ｊ≦ｔのいずれかであり、それぞれの器は、ｔ＋１回処理を行う。
（４）　乱数発生器６０７
出力：対称鍵ＤＥＫ（ランダム生成）
（５）　電子署名生成・連結器６０６
入力：Ｍ［０］又はＭ［ｊ］、Ａの署名用秘密鍵ＳＫｓＡ
出力：Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］））　（ｊ＝０、…、ｔ）
ハッシュダイジェストｈ（Ｍ［ｊ］）の生成
電子署名ＳＫｓＡ（ｈ（Ｍ［ｊ］））の生成
Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］））：入力と電子署名の連結
（６）　暗号器６０８
入力：電子署名付き本文Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］））、対称鍵ＤＥＫ
出力：暗号化データＤＥＫ（Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］）））　（ｊ＝０、…、ｔ）
（７）　複数人暗号器６０９
入力：対称鍵ＤＥＫ、複数の暗号化鍵Ｅｎｃ-Ａ-Ｂ［ｉ］（ｉ＝１、…、ｎ）
出力：暗号化データＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）（ｉ＝１、…、ｎ）
複数の復号化装置を対象に暗号化する。
【００４０】（８）　暗号データ連結器６１０
入力：全暗号化データＤＥＫ（Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］）））（ｊ＝０、…、ｔ）及びＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）（ｉ＝１、…、ｎ）
出力：暗号文Ｃ
暗号化データ全てを連結し、一つにまとめる。
【００４１】図５は図２のステップ７に対応した暗号化装置Ａによるグループ暗号化ファイル作成の一例を示す説明図であり、図６及び図７は図２のステップ７に対応した暗号化装置Ａの処理フロー図である。
【００４２】すなわち、先ず、ファイルの暗号化について説明する。暗号化前にファイルＦ［ｊ］（ｊ＝１、…、ｔ）を選択してファイル情報分離器６０１に入力する。ファイル情報分離器６０１は入力されたファイルＦ［ｊ］をファイル情報Ｍ［０］とファイル内容Ｍ［ｊ］（ｊ＝１、…、ｔ）に分離して電子署名生成・連結器６０６に出力する。一方、暗号化前に決定済の暗号化装置利用者名Ａはグループ情報変換器６０２に入力され、このグループ情報変換器６０２はグループ情報ＤＢ６０３を参照して暗号化装置利用者名Ａを変換し、暗号化装置名Ａを取得して鍵検索器６０４に出力する。この鍵検索器６０４は要求元の電子署名生成・連結器６０６の情報に応じて鍵ＤＢ６０５を参照して暗号化装置名Ａの署名用秘密鍵ＳＫｓＡを検索・取得して電子署名生成・連結器６０６に出力する。この電子署名生成・連結器６０６はファイル情報とファイル内容Ｍ［ｊ］（ｊ＝０、…、ｔ）に電子署名を生成して付加したＭ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］））　（ｊ＝０、…、ｔ）を暗号器６０８に出力する。この暗号器６０８には乱数発生器６０７でランダムに生成された対称鍵ＤＥＫが入力され、前記電子署名生成・連結器６０６から入力されたＭ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］））　（ｊ＝０、…、ｔ）を対称鍵ＤＥＫで暗号化したファイルの暗号化データＤＥＫ（Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］）））　（ｊ＝０、…、ｔ）を暗号データ連結器６１０に出力する。
【００４３】次に、対称鍵の暗号化について説明する。暗号化前に選択済の復号化装置利用グループ名Ｇはグループ情報変換器６０２に入力され、このグループ情報変換器６０２はグループ情報ＤＢ６０３を参照して復号化装置利用グループ名Ｇを各復号化装置名Ｂ［ｉ］（ｉ＝１、…、ｎ）へ変換して鍵検索器６０４に出力する。この鍵検索器６０４は要求元の複数人暗号器６０９の情報に応じて鍵ＤＢ６０５を参照して暗号化装置Ａと復号化装置Ｂ［ｉ］（ｉ＝１、…、ｎ）の間の暗号化鍵Ｅｎｃ-Ａ-Ｂ［ｉ］を全て検索・取得して複数人暗号器６０９に出力する。この複数人暗号器６０９には乱数発生器６０７でランダムに生成された対称鍵ＤＥＫが入力され、この対称鍵ＤＥＫを暗号化鍵Ｅｎｃ-Ａ-Ｂ［ｉ］で暗号化した対称鍵の暗号化データＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）を暗号データ連結器６１０に出力する。
【００４４】前記暗号データ連結器６１０は暗号器６０８から入力されたファイルの暗号化データＤＥＫ（Ｍ

［j］‖ＳＫｓＡ（ｈ（Ｍ［j］））　（ｊ＝0、…、ｔ）及び複数人暗号器６０９から入力された対称鍵の暗号化データＥｎｃ-Ａ-Ｂ　［ｉ］（ＤＥＫ）全体を連結し、暗号文Ｃを生成する。

【００４５】図５に示すように、前記ファイル情報Ｍ［0］とファイル内容Ｍ［j］（ｊ＝１、…、ｔ）は送信者の暗号化装置Ａの署名用秘密鍵ＳＫｓＡで電子署名される。また、電子署名付ファイル情報と電子署名付ファイル内容は対称鍵ＤＥＫで暗号化される。さらに、対称鍵ＤＥＫは送信者の暗号化装置Ａの秘密鍵ＳＫｄＡ及び受信者の復号化装置Ｂ［ｉ］（ｉ＝１、…、ｎ）の公開鍵ＰＫｄＢ［ｉ］（ｉ＝１、…、ｎ）を用いて暗号化される。

【００４６】尚、暗号化装置Ａを復号化対象に含めるか否かは任意である。暗号化装置Ａを復号化対象に含めた場合でも、同様に暗号化可能である。Ｂ［1］＝Ａとなる。図８は図２のステップ１２に対応した復号化装置Ｂ［ｉ］（ｉ＝１、…、ｎ）のファイル情報復号化部分の一例を示す構成説明図である。図８の各部を説明する。

【００４７】（1）．暗号データ分離器７０１

入力：暗号文Ｃ

出力：全暗号化データＤＥＫ（Ｍ［j］‖ＳＫｓＡ（ｈ（Ｍ［j］））（ｊ＝0、…、ｔ）及びＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）（ｉ＝１、…、ｎ）

暗号文Ｃを（カッコの外の‖ごとに）暗号化データに分離する。

【００４８】（2）　鍵検索器７０２、鍵ＤＢ７０３

入力：装置名、要求元（鍵の要求元の情報。複数人復号器７０４からの暗号化装置名Ａまたは電子署名分離・検証器７０６からの要求情報）

出力：公開鍵方式の鍵（複数人復号器７０４へ復号化鍵Ｄｅｃ-Ａ-Ｂ［ｉ］または電子署名分離・検証器７０６へ暗号化装置名Ａの署名用公開鍵ＰＫｓＡ）鍵ＤＢ７０３には、装置名とその公開鍵が格納されている。入力を基に、鍵ＤＢ７０３から秘密鍵・公開鍵を取り出して、必要に応じて復号化鍵を生成し、要求元（複数人復号器７０４や電子署名分離・検証器７０６）へ渡す。

【００４９】（3）　複数人復号器７０４

入力：暗号化データＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）（ｉ＝１、…、ｎ）または復号化鍵Ｄｅｃ-Ａ-Ｂ［ｉ］

出力：対称鍵ＤＥＫ

暗号化データＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）（ｉ＝１、…、ｎ）から、復号化装置Ｂ［ｉ］向けの暗号化データＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）を選び出し、復号化鍵Ｄｅｃ-Ａ-Ｂ［ｉ］で復号化し、対称鍵ＤＥＫを取得する。

【００５０】（4）　復号器７０５

入力：暗号化データＤＥＫ（Ｍ［0］‖ＳＫｓＡ（ｈ（Ｍ［0］））および対称鍵ＤＥＫ

出力：電子署名付き本文Ｍ［0］‖ＳＫｓＡ（ｈ（Ｍ［0］））

（5）　電子署名分離・検証器７０６

入力：電子署名付き本文Ｍ［0］‖ＳＫｓＡ（ｈ（Ｍ［0］））、暗号化装置名Ａの署名用公開鍵ＰＫｓＡ

出力：ファイル情報Ｍ［0］

Ｍ［0］．ＳＫｓＡ（ｈ（Ｍ［0］））：入力と電子署名の分離

ハッシュダイジェストｈ１＝ｈ（Ｍ［0］）の生成

ｈ２＝ｈ（Ｍ［0］）＝ＰＫｓＡ（ＳＫｓＡ（ｈ（Ｍ［0］））：電子署名ＳＫｓＡ（ｈ（Ｍ［0］））の復号化

署名の検証（ｈ１＝ｈ２か否か）

ｈ１＝ｈ２→ＯＫ．Ｍ［0］を取得

ｈ１≠ｈ２→ＮＧ．処理を中断

（6）　表示装置７０８

入力：ファイル情報Ｍ［0］

出力：ファイル情報Ｍ［0］

復号化するファイル内容Ｍ［j］を選択させるため（図９の入力に反映）、ファイル情報Ｍ［0］を表示する。

【００５１】（7）　一時的記憶装置７０７

入力：ファイル情報Ｍ［0］、対称鍵ＤＥＫ、暗号化データＤＥＫ（Ｍ［j］‖ＳＫｓＡ（ｈ（Ｍ［j］）））（ｊ＝１、…、ｔ）

選択されたファイル内容Ｍ［j］を復号化するために必要な、データを格納しておく。

【００５２】図９は図２のステップ１２に対応した復号化装置Ｂ［ｉ］（ｉ＝１、…、ｎ）のファイル内容復号化部分の一例を示す構成説明図である。図９の各部を説明する。

【００５３】（1）　入力装置８０１

入力：インデックスｊ［1］、…、ｊ［ｕ］（表示情報から復号化の対象として選択されたファイルの番号）

出力：インデックスｊ［1］、…、ｊ［ｕ］

表示装置７０８（図８参照）の情報を基に、利用者がファイルを選択した結果を得、以降の処理で使用される。

【００５４】（2）　一時的記憶装置８０２（図８の一時的記憶装置７０７と同一）

入力：インデックスｊ［1］、…、ｊ［ｕ］

出力：ファイル情報Ｍ［0］、対称鍵ＤＥＫ、入力装置８０１で選択されたファイルの番号に対応した暗号化データＤＥＫ（Ｍ［j］‖ＳＫｓＡ（ｈ（Ｍ［j］）））（ｊ＝ｊ［1］、…、ｊ［ｕ］）

選択されたＭ［j］を復号化するために必要なデータを他の器へ受け渡す。

【００５５】（3）　復号器８０３

入力：暗号化データＤＥＫ（Ｍ［j］‖ＳＫｓＡ（ｈ（Ｍ［j］））（ｊ＝ｊ［1］、…、ｊ［ｕ］）および対称鍵ＤＥＫ

出力：電子署名付き本文Ｍ［j］‖ＳＫｓＡ（ｈ（Ｍ［j］））（ｊ＝ｊ［1］、…、ｊ［ｕ］）

（4） 鍵検索器８０５、鍵ＤＢ８０６
入力：装置名（図８で入力済）、要求元（鍵の要求元の情報。電子署名分離・検証器８０４からの情報）
出力：公開鍵方式の鍵。暗号化装置名Ａの署名用公開鍵ＰＫｓＡ
鍵ＤＢ８０６には、装置名とその公開鍵が格納されている。入力を基に、鍵ＤＢ８０６から秘密鍵・公開鍵を取り出して、必要に応じて復号化鍵を生成し、要求元（電子署名分離・検証器８０４）へ渡す。
【００５６】以降現れる単独のｊは、ｊ［１］、…、ｊ［ｕ］のいずれか値であり、取り得る値は１≦ｊ≦ｔである。それぞれの器は、ｕ回処理を行う。
【００５７】（５） 電子署名分離・検証器８０４
入力：Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］））（ｊ＝ｊ［１］、…、ｊ［ｕ］）、暗号化装置名Ａの署名用公開鍵ＰＫｓＡ
出力：ファイル内容Ｍ［ｊ］（ｊ＝ｊ［１］、…、ｊ［ｕ］）
Ｍ［ｊ］．ＳＫｓＡ（ｈ（Ｍ［ｊ］））：入力と電子署名の分離
ハッシュダイジェストｈ１＝ｈ（Ｍ［ｊ］）の生成
ｈ２＝ｈ（Ｍ［ｊ］）＝ＰＫｓＡ（ＳＫｓＡ（ｈ（Ｍ［ｊ］）））：電子署名ＳＫｓＡ（ｈ（Ｍ［ｊ］））の復号化
署名の検証（ｈ１＝ｈ２か否か）
ｈ１＝ｈ２→ＯＫ．Ｍ［ｊ］を取得
ｈ１≠ｈ２→ＮＧ．処理を中断もしくはスキップ（次の暗号化データを処理）
（６） ファイル情報連結器８０７
入力：ファイル情報Ｍ［０］およびファイル内容Ｍ［ｊ［１］］、…、Ｍ［ｊ［ｕ］］
出力：ファイルＦ［ｊ［１］］、…、Ｆ［ｊ［ｕ］］
選択されたファイルのみ、ファイル情報とファイル内容からファイルを再構築する。
【００５８】図１０は図２のステップ１２に対応した復号化装置Ｂ［ｉ］（ｉ＝１、…、ｎ）によるグループ暗号化ファイルの復号化の一例を示す説明図であり、図１１及び図１２は図２のステップ１２に対応した復号化装置Ｂ［ｉ］（ｉ＝１、…、ｎ）の処理フロー図である。
【００５９】すなわち、先ず、ファイル情報の復号化について説明する。図８、図１０および図１１に示すように、暗号データ分離器７０１は入力された暗号文Ｃを暗号化部分ごとに分離し、全暗号化データＤＥＫ（Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］）））（ｊ＝０、…、ｔ）及びＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）（ｉ＝１、…、ｎ）を取得し、暗号化データＤＥＫ（Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］）））（ｊ＝１、…、ｔ）は一時的記憶装置７０７に格納し、暗号化データＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）（ｉ＝１、…、ｎ）は複数人復号器７０４に出力し、暗号化データＤＥＫ（Ｍ［０］‖ＳＫｓＡ（ｈ（Ｍ［０］））は復号器７０５に出力する。複数人復号器７０４は鍵検索器７０２、鍵ＤＢ７０３に要求して暗号化装置Ａと復号化装置Ｂ［ｉ］の間の復号化鍵Ｄｅｃ-Ａ-Ｂ［ｉ］を検索、取得し、暗号化データＥｎｃ-Ａ-Ｂ［ｉ］（ＤＥＫ）を復号化鍵Ｄｅｃ-Ａ-Ｂ［ｉ］で復号化し、対称鍵ＤＥＫを取得し、この対称鍵ＤＥＫを一時的記憶装置７０７に格納すると共に復号器７０５に出力する。この復号器７０５は暗号化データＤＥＫ（Ｍ［０］‖ＳＫｓＡ（ｈ（Ｍ［０］））を対称鍵ＤＥＫで復号化し、Ｍ［０］‖ＳＫｓＡ（ｈ（Ｍ［０］））（Ｍ［０］とＡの電子署名）を取得し、電子署名分離・検証器７０６に出力する。電子署名分離・検証器７０６は鍵検索器７０２、鍵ＤＢ７０３に要求して暗号化装置Ａの署名用公開鍵ＰＫｓＡを検索、取得する。電子署名分離・検証器７０６はＳＫｓＡ（ｈ（Ｍ［０］））（Ａの電子署名）を検証し、電子署名が間違っていれば（ＮＧ）、エラー処理し、処理を中断する。一方、電子署名が正しければ（ＯＫ）、ファイル情報Ｍ［０］を取得し、このファイル情報Ｍ［０］を一時的記憶装置７０７に格納すると共に表示装置７０８に出力する。表示装置７０８はファイル情報Ｍ［０］を表示して出力する。
【００６０】次に、ファイル内容の復号化について説明する。図９、図１０および図１２に示すように、入力装置８０１には表示装置７０８（図８参照）に表示されているファイル情報Ｍ［０］を基にしてファイルの番号であるインデックスｊ［１］、…、ｊ［ｕ］が選択されて入力され、このインデックスｊ［１］、…、ｊ［ｕ］は一時的記憶装置８０２に出力される。この一時的記憶装置８０２には一時的記憶装置７０７（図８参照）と同様にファイル情報Ｍ［０］、暗号化データＤＥＫ（Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］）））（ｊ＝１、…、ｔ）、及び対称鍵ＤＥＫが格納されており、前記ファイル情報Ｍ［０］は読み出されてファイル情報連結器８０７に入力され、前記暗号化データＤＥＫ（Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］）））（ｊ＝１、…、ｔ）、及び対称鍵ＤＥＫは読み出されて復号器８０３に入力される。この復号器８０３は暗号化データＤＥＫ（Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］）））（ｊ＝１、…、ｔ）を対称鍵ＤＥＫで復号化し、Ｍ［ｊ］‖ＳＫｓＡ（ｈ（Ｍ［ｊ］））（Ｍ［ｊ］とＡの電子署名）を取得して電子署名分離・検証器８０４に出力する。電子署名分離・検証器８０４は鍵検索器８０５、鍵ＤＢ８０６に要求して暗号化装置Ａの署名用公開鍵ＰＫｓＡを検索、取得する。前記電子署名分離・検証器８０４はＳＫｓＡ（ｈ（Ｍ［ｊ］））（Ａの電子署名）を検証し、電子署名が間違っていれば（ＮＧ）、エラー処理し、処理を中断もしくはスキップして次のＭ［ｊ］に対する処理を行う。一方、電子署名が正しければ（ＯＫ）、ファイル内容Ｍ［ｊ］（ｊ＝ｊ［１］、…、ｊ［ｕ］）を取得してファ

イル情報連結器８０７に出力する。このファイル情報連結器８０７はファイル情報Ｍ［０］及びファイル内容Ｍ［ｊ］（ｊ＝ｊ［１］、…、ｊ［ｕ］）からファイルＦ［ｊ］（ｊ＝ｊ［１］、…、ｊ［ｕ］）を生成して出力する。

【００６１】図１０に示すように、暗号化された対称鍵ＤＥＫは送信者の暗号化装置Ａの公開鍵（楕円ＤＨ）ＰＫｄＡ及び受信者の復号化装置Ｂ［ｉ］（ｉ＝１、…、ｎ）の秘密鍵ＳＫｄＢ［ｉ］（ｉ＝１、…、ｎ）を用いて復号化される。また、暗号化された電子署名付ファイル情報とファイル内容は対称鍵ＤＥＫで復号化される。さらに、電子署名付ファイル情報と電子署名付ファイル内容は送信者の暗号化装置Ａの署名用公開鍵ＰＫｓＡで電子署名が分離・検証される。

【００６２】尚、送信者が暗号化したファイルと暗号化した対称鍵を記録媒体に記録して受信者に渡すようにしてもよい。又、少なくとも公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するようにしてもよい。

【００６３】本発明の実施形態には次の発明が含まれる。

（１）　ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を送信するステップとを少なくとも持つことを特徴とする暗号化方法。

【００６４】（２）　ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化方法であって、対称鍵を用いて該ファイルを暗号化するステップと、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化するステップと、前記暗号化したファイルと前記暗号化した対称鍵を記録媒体に記録して受信者へ渡すステップとを少なくとも持つことを特徴とする暗号化方法。

【００６５】（３）　前記ファイルに関する情報を対称鍵を用いて暗号化するステップを持つことを特徴とする上記（１）又は（２）記載の暗号化方法。

（４）　前記ファイル内容及びファイルに関する情報に電子署名情報を付与することを特徴とする上記（３）記載の暗号化方法。

【００６６】（５）　少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする上記（１）、（２）、（３）又は（４２）記載の暗号化方法。

【００６７】（６）　暗号化されたファイル及び対称鍵を復号化する復号化方法であって、前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、該復号化された対称鍵を用いて前記暗号化されたファイルを復号化するステップとを少なくとも持つことを特徴とする復号化方法。

【００６８】（７）　暗号化されたファイル及び対称鍵を復号化する復号化方法であって、前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化するステップと、該復号化された対称鍵を用いて前記暗号化されたファイルを復号化するステップと、復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定するステップを持つことを特徴とする復号化方法。

【００６９】（８）　少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手することを特徴とする上記（６）又は（７）記載の復号化方法。

【００７０】（９）　対称鍵を発生する対称鍵発生手段と、この対称鍵発生手段で発生した対称鍵でファイルを暗号化するファイル暗号化手段と、前記対称鍵発生手段で発生した対称鍵を送信者の秘密鍵と受信者の公開鍵で暗号化する対称鍵暗号化手段と、この対称鍵暗号化手段で暗号化した対称鍵と前記ファイル暗号化手段で暗号化したファイルを連結する連結手段とを具備することを特徴とする暗号化装置。

【００７１】（１０）　対称鍵を発生する対称鍵発生手段と、この対称鍵発生手段で発生した対称鍵でファイルを暗号化するファイル暗号化手段と、前記対称鍵発生手段で発生した対称鍵でファイルに関する情報を暗号化するファイル情報暗号化手段と、前記対称鍵発生手段で発生した対称鍵を送信者の秘密鍵と受信者の公開鍵で暗号化する対称鍵暗号化手段と、この対称鍵暗号化手段で暗号化した対称鍵と前記ファイル暗号化手段で暗号化したファイルと前記ファイル情報暗号化手段で暗号化したファイルに関する情報を連結する連結手段とを具備することを特徴とする暗号化装置。

【００７２】（１１）　ファイル内容及びファイルに関する情報に送信者の署名用秘密鍵で電子署名情報を付与する電子署名手段を具備することを特徴とする上記（９）又は（１０）記載の暗号化装置。

【００７３】（１２）　暗号データから暗号化された対称鍵と暗号化されたファイルを分離する暗号データ分離手段と、この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイルを復号化するファイル復号化手段とを具備することを特徴とする復号化装置。

【００７４】（１３）　暗号データから暗号化された対称鍵と暗号化された電子署名付ファイルを分離する暗号データ分離手段と、この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用

いて復号化する対称鍵復号化手段と、この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルを復号化するファイル復号化手段と、このファイル復号化手段で復号化された電子署名付ファイルを送信者の署名用公開鍵を用いて電子署名を分離して検証する電子署名分離・検証手段とを具備することを特徴とする復号化装置。

【００７５】（１４） 暗号データから暗号化された対称鍵と暗号化されたファイルに関する情報と暗号化されたファイル内容を分離する暗号データ分離手段と、この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイル情報を復号化するファイル情報復号化手段と、前記対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化ファイルを復号化するファイル復号化手段とを具備することを特徴とする復号化装置。

【００７６】（１５） 暗号データから暗号化された対称鍵と暗号化された電子署名付ファイルに関する情報と暗号化された電子署名付ファイルを分離する暗号データ分離手段と、この暗号データ分離手段で分離された暗号化対称鍵を送信者の公開鍵と受信者の秘密鍵を用いて復号化する対称鍵復号化手段と、この対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイル情報を復号化するファイルに関する情報復号化手段と、前記対称鍵復号化手段で復号化された対称鍵を用いて前記暗号データ分離手段で分離された暗号化電子署名付ファイルを復号化するファイル復号化手段と、このファイル復号化手段で復号化された電子署名付ファイルと前記ファイル情報復号化手段で復号化された電子署名付ファイル情報を送信者の署名用公開鍵を用いて電子署名を分離して検証する電子署名分離・検証手段とを具備することを特徴とする復号化装置。

【００７７】（１６） 復号化されたファイル情報に基づいて所定のファイルを選択して復号化するファイル選択手段を具備することを特徴とする上記（１４）又は（１５）記載の復号化装置。

【００７８】（１７） ファイルの送信者が１人又は複数の受信者へ該ファイルを配布するための暗号化プログラムを記録した記録媒体であって、対称鍵を用いて該ファイルを暗号化する手順、該対称鍵を送信者の秘密鍵と受信者の公開鍵を用いて暗号化する手順、前記暗号化したファイルと前記暗号化した対称鍵を送信する手順を実行させるための暗号化プログラムを記録した記録媒体。

【００７９】（１８） 前記ファイルに関する情報を対称鍵を用いて暗号化する手順を実行させるためのプログラムを記録したことを特徴とする上記（１７）記載の暗号化プログラムを記録した記録媒体。

【００８０】（１９） 前記ファイル及びファイルに関する情報に電子署名情報を付与するためのプログラムを記録したことを特徴とする上記（１８）記載の暗号化プログラムを記録した記録媒体。

【００８１】（２０） 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するためのプログラムを記録したことを特徴とする上記（１７）、（１８）、又は（１９）記載の暗号化プログラムを記録した記録媒体。

【００８２】（２１） 暗号化されたファイル内容又はファイルに関する情報及び対称鍵を復号化するためのプログラムを記録した記録媒体であって、前記送信者から送信された前記暗号化された対称鍵を前記送信者の公開鍵と前記受信者の秘密鍵を用いて復号化する手順、該復号化された対称鍵を用いて前記暗号化されたファイル内容又はファイルに関する情報を復号化する手順を実行させるための復号化プログラムを記録した記録媒体。

【００８３】（２２） 前記復号化されたファイルに関する情報に基づき受信者側で復号化すべきファイルを指定する手順を実行させるためのプログラムを記録したことを特徴とする上記（２１）記載の復号化プログラムを記録した記録媒体。

【００８４】（２３） 少なくとも前記公開鍵を認証サーバから通信ネットワークを介して又は認証機関から入手するためのプログラムを記録したことを特徴とする上記（２１）又は（２２）記載の復号化プログラムを記録した記録媒体。

【００８５】（２４） ファイルの所有者が複数の閲覧者（所有者を含む）へ該ファイルを暗号化する方法であって、対称鍵を用いて前記ファイルを暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、前記暗号化したファイルと該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【００８６】（２５） ファイルの所有者が複数の閲覧者（所有者を含む）へファイルの内容と該ファイルに関する情報を暗号化する方法であって、該ファイルを該ファイル内容と該ファイルに関する情報に分離するステップと、対称鍵を用いて前記ファイル内容と前記ファイルに関する情報を暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【００８７】（２６） ファイルの所有者が複数の閲覧者（所有者を含む）へ該ファイルを暗号化する方法であって、前記所有者が前記閲覧者の情報を任意のグループ

に分けて管理するステップと、該グループから、前記グループに属する閲覧者の情報を抽出するステップと、前記閲覧者の情報から前記閲覧者の公開鍵をを抽出するステップと、対称鍵を用いて前記ファイルを暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、前記暗号化したファイルと該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【００８８】（２７） ファイルの所有者が複数の閲覧者（所有者を含む）へファイル内容と該ファイルに関する情報を暗号化する方法であって、前記所有者が前記閲覧者の情報を任意のグループに分けて管理するステップと、該グループから、前記グループに属する閲覧者の情報を抽出するステップと、前記閲覧者の情報から前記閲覧者の公開鍵をを抽出するステップと、該ファイルを該ファイル内容と該ファイルに関する情報に分離するステップと、対称鍵を用いて前記ファイル内容と前記ファイルに関する情報を暗号化するステップと、該対称鍵を該所有者の秘密鍵と該閲覧者の公開鍵を用いて前記複数の閲覧者の数分だけ暗号化済対称鍵を生成するステップと、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と該暗号化済対称鍵全てを結合するステップとを少なくとも持つことを特徴とする暗号化方法。

【００８９】（２８） 暗号化したファイルと暗号化済対称鍵全てを結合したものを復号化する方法であって、前記暗号化したファイルと暗号化済対称鍵全てを結合したものから、前記暗号化したファイルと暗号化済対称鍵全てを分離するステップと、所有者の公開鍵と閲覧者の秘密鍵を用いて前記暗号化済対称鍵を復号化するステップと、該復号化された対称鍵を用いて該暗号化したファイルを復号化するステップとを少なくとも持つことを特徴とする復号化方法。

【００９０】（２９） 暗号化したファイル内容と暗号化したファイルに関する情報と暗号化済対称鍵全てを結合したものを復号化する方法であって、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と暗号化済対称鍵全てを結合したものから、前記暗号化したファイル内容と前記暗号化したファイルに関する情報と暗号化済対称鍵全てを分離するステップと、所有者の公開鍵と閲覧者の秘密鍵を用いて前記暗号化済対称鍵を復号化するステップと、該復号化された対称鍵を用いて該暗号化したファイル内容と該暗号化したファイルに関する情報を復号化するステップと、該復号化されたファイル内容と該復号化されたファイルに関する情報を結合し前記ファイルを再構成するステップとを少なくとも持つことを特徴とする復号化方法。

【００９１】（３０） 復号化されたファイルに関する情報に基き、閲覧者側で復号化すべきファイルを指定するステップと、復号化された対称鍵を用いて暗号化したファイルのうち指定された該復号化すべきファイルを復号化するステップとを持つことを特徴とする復号化方法。

【００９２】（３１） 所有者の秘密鍵を用いて前記ファイルの電子署名を生成するステップと、前記ファイルに該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【００９３】（３２） 所有者の秘密鍵を用いて前記ファイル内容の電子署名を生成するステップと、前記ファイル内容に該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【００９４】（３３） 所有者の秘密鍵を用いて前記ファイルに関する情報の電子署名を生成するステップと、前記ファイルに関する情報に該電子署名を結合するステップとを持つことを特徴とする電子署名方法。

【００９５】（３４） ファイルから電子署名を分離するステップと、所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【００９６】（３５） ファイル内容から電子署名を分離するステップと、所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【００９７】（３６） ファイルに関する情報から電子署名を分離するステップと、所有者の公開鍵を用いて前記電子署名の検証を行うステップとを持つことを特徴とする電子署名検証方法。

【００９８】

【発明の効果】以上述べたように本発明によれば、個人が持つ１つの秘密鍵、認証機関（ＣＡ）に公開されている１つの公開鍵という形態のままで公開鍵方式のグループ暗号を実現することにより、鍵配送が安全でかつ簡単であり、さらに任意のグループを簡単に作成する事ができる暗号化方法及び装置、復号化方法及び装置、暗号化プログラムを記録した記録媒体、復号化プログラムを記録した記録媒体、電子署名方法、並びに電子署名検証方法を提供することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態例を示す概略構成説明図である。

【図２】本発明の一実施形態例に係る認証機関を介する場合の各装置間のフロー図である。

【図３】本発明の一実施形態例に係る認証機関を介さない場合の各装置間のフロー図である。

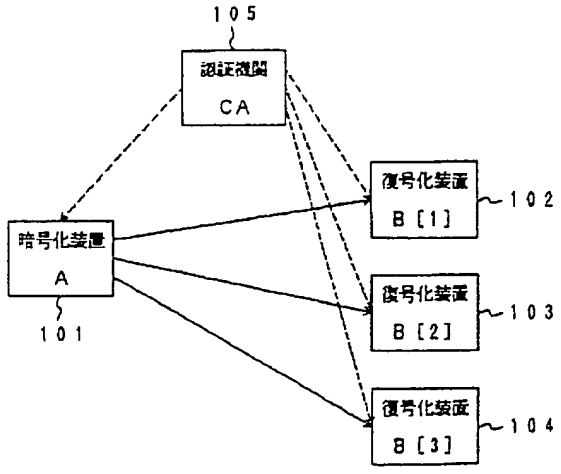
【図４】本発明の一実施形態例に係る暗号化装置を示す構成説明図である。

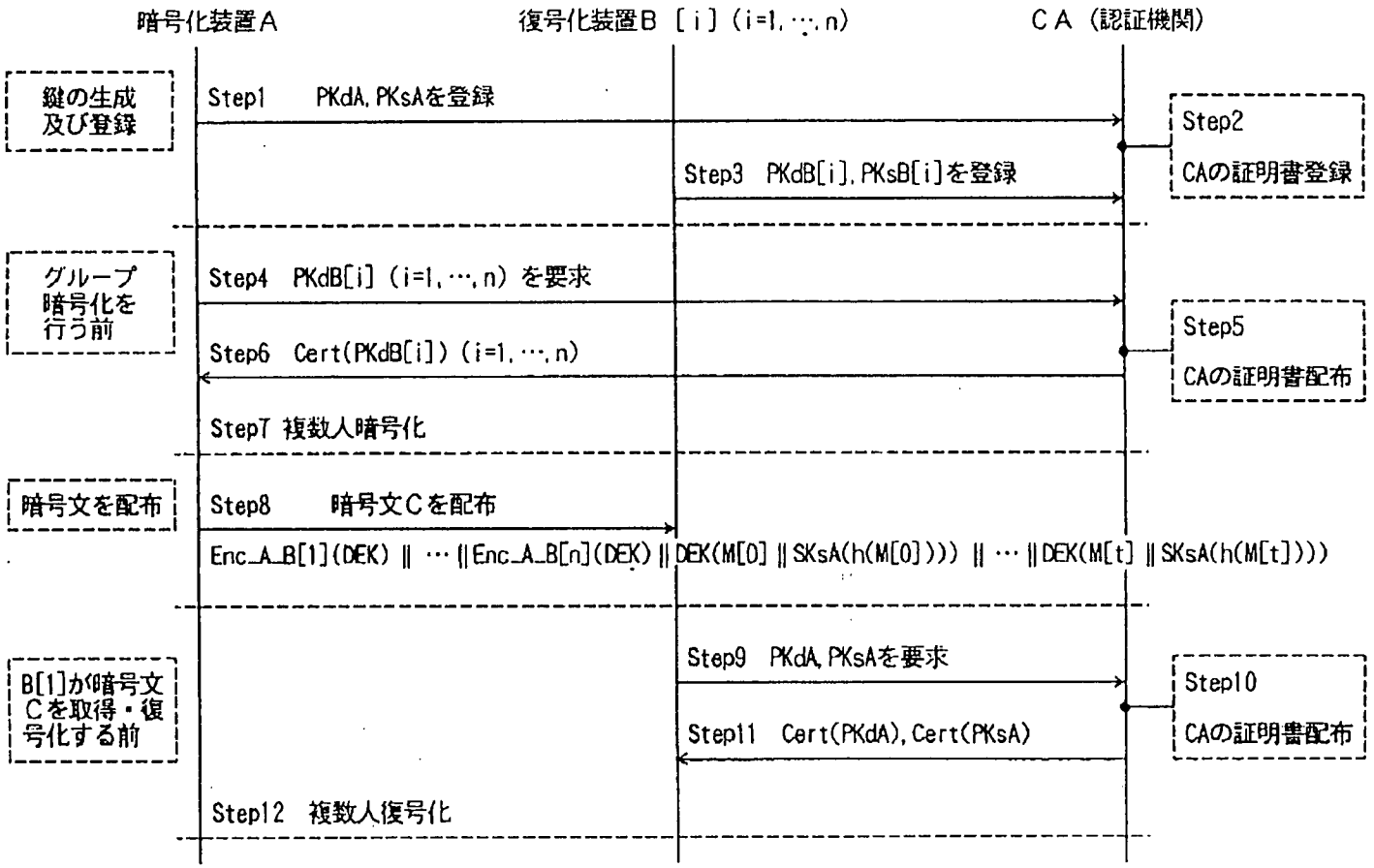
【図５】本発明の一実施形態例に係る暗号化装置のグループ暗号化ファイル作成を示す説明図である。

【図６】本発明の一実施形態例に係る暗号化装置の暗号

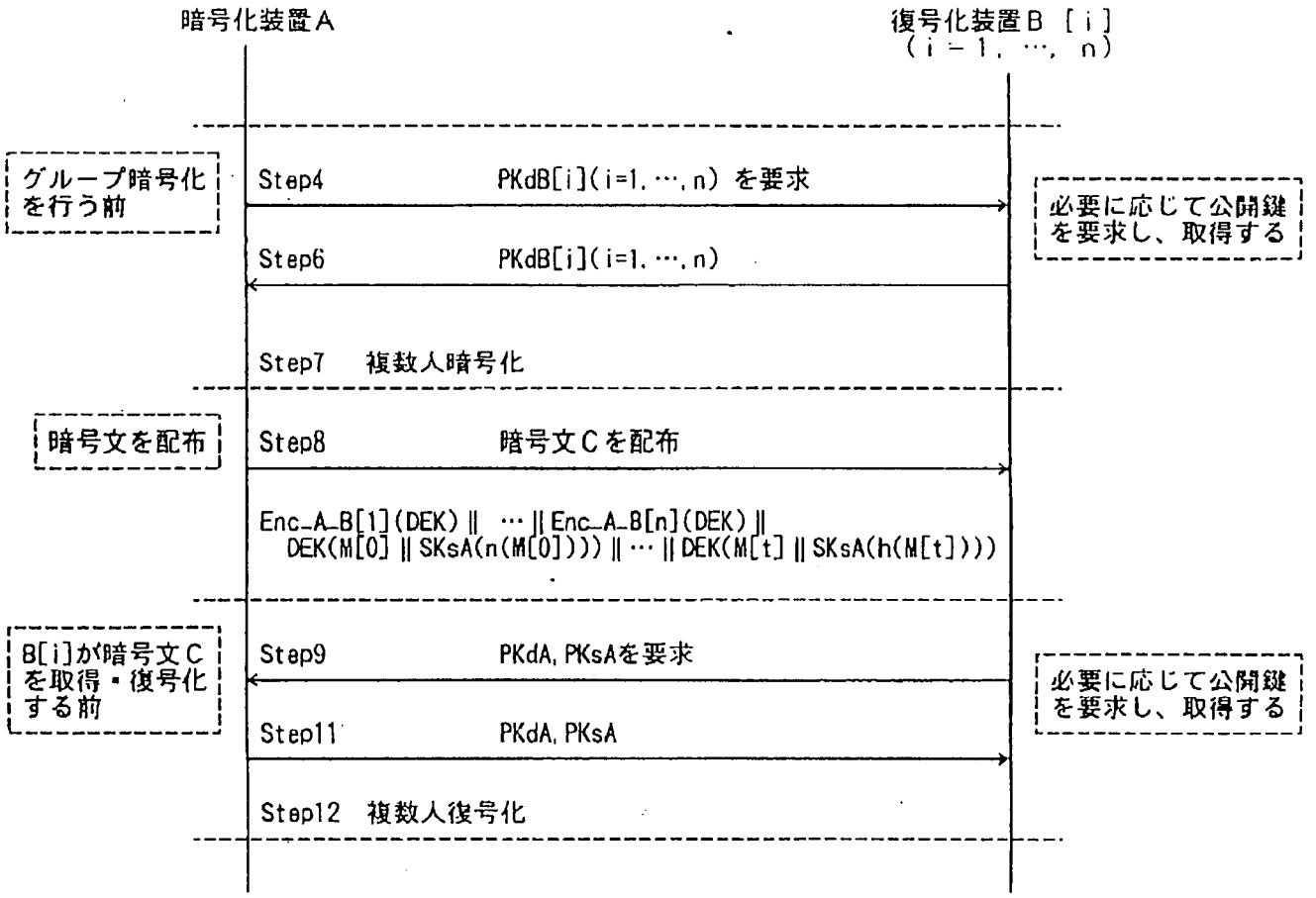
化ファイル作成を示すフロー図である。
【図７】本発明の一実施形態例に係る暗号化装置の暗号化対称鍵作成を示すフロー図である。
【図８】本発明の一実施形態例に係る復号化装置のファイル情報復号化部分を示す構成説明図である。
【図９】本発明の一実施形態例に係る復号化装置のファイル内容復号化部分を示す構成説明図である。
【図１０】本発明の一実施形態例に係る復号化装置のグループ復号化ファイル作成を示す説明図である。
【図１１】本発明の一実施形態例に係る復号化装置のファイル情報復号化部分を示すフロー図である。
【図１２】本発明の一実施形態例に係る復号化装置のファイル内容復号化部分を示すフロー図である。
【符号の説明】
１０１　送信者の暗号化装置Ａ
１０２　受信者の復号化装置Ｂ［１］
１０３　受信者の復号化装置Ｂ［２］
１０４　受信者の復号化装置Ｂ［３］
１０５　認証機関ＣＡ
６０１　ファイル情報分離器
６０２　グループ情報変換器
６０３　グループ情報ＤＢ
６０４　鍵検索器
６０５　鍵ＤＢ
６０６　電子署名生成・連結器
６０７　乱数発生器
６０８　暗号器
６０９　複数人暗号器
６１０　暗号データ連結器
７０１　暗号データ分離器
７０２　鍵検索器
７０３　鍵ＤＢ
７０４　複数人復号器
７０５　復号器
７０６　電子署名分離・検証器
７０７　一時的記憶装置
７０８　表示装置
８０１　入力装置
８０２　一時的記憶装置
８０３　復号器
８０４　電子署名分離・検証器
８０５　鍵検索器
８０６　鍵ＤＢ
８０７　ファイル情報連結器

【図１】



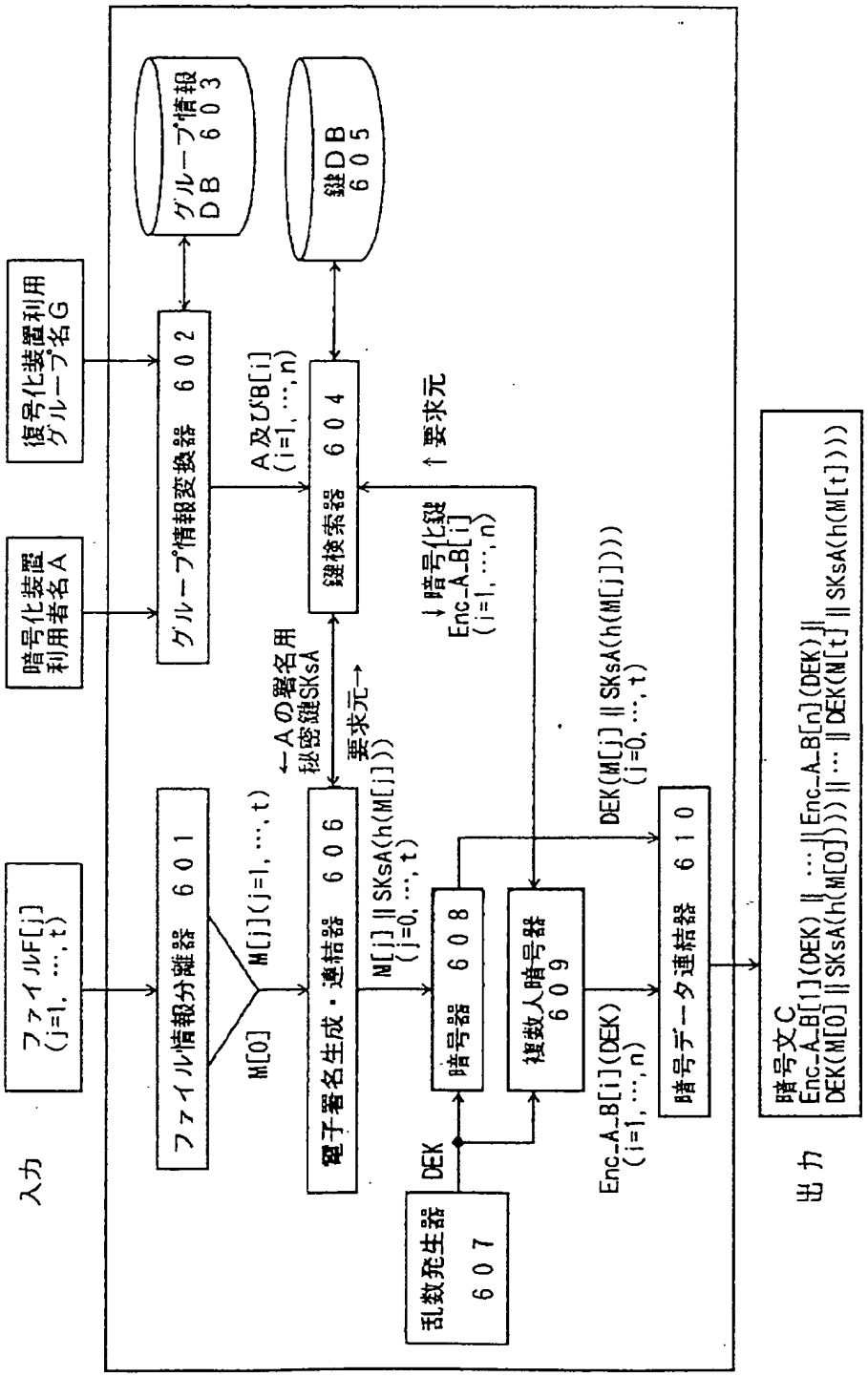

暗号化装置A
復号化装置B［i］(i=1, …, n)
CA（認証機関）
鍵の生成及び登録
Step1　PKdA, PKsAを登録
Step2
CAの証明書登録
Step3　PKdB[i], PKsB[i]を登録
グループ暗号化を行う前
Step4　PKdB[i]（i=1, …, n）を要求
Step5
CAの証明書配布
Step6　Cert(PKdB[i])（i=1, …, n）
Step7 複数人暗号化
暗号文を配布
Step8　暗号文Cを配布
Enc_A_B[1](DEK) ‖ … ‖Enc_A_B[n](DEK) ‖ DEK(M[0] ‖ SKsA(h(M[0]))) ‖ … ‖ DEK(M[t] ‖ SKsA(h(M[t])))
B[1]が暗号文Cを取得・復号化する前
Step9　PKdA, PKsAを要求
Step10
CAの証明書配布
Step11　Cert(PKdA), Cert(PKsA)
Step12　複数人復号化

【図2】

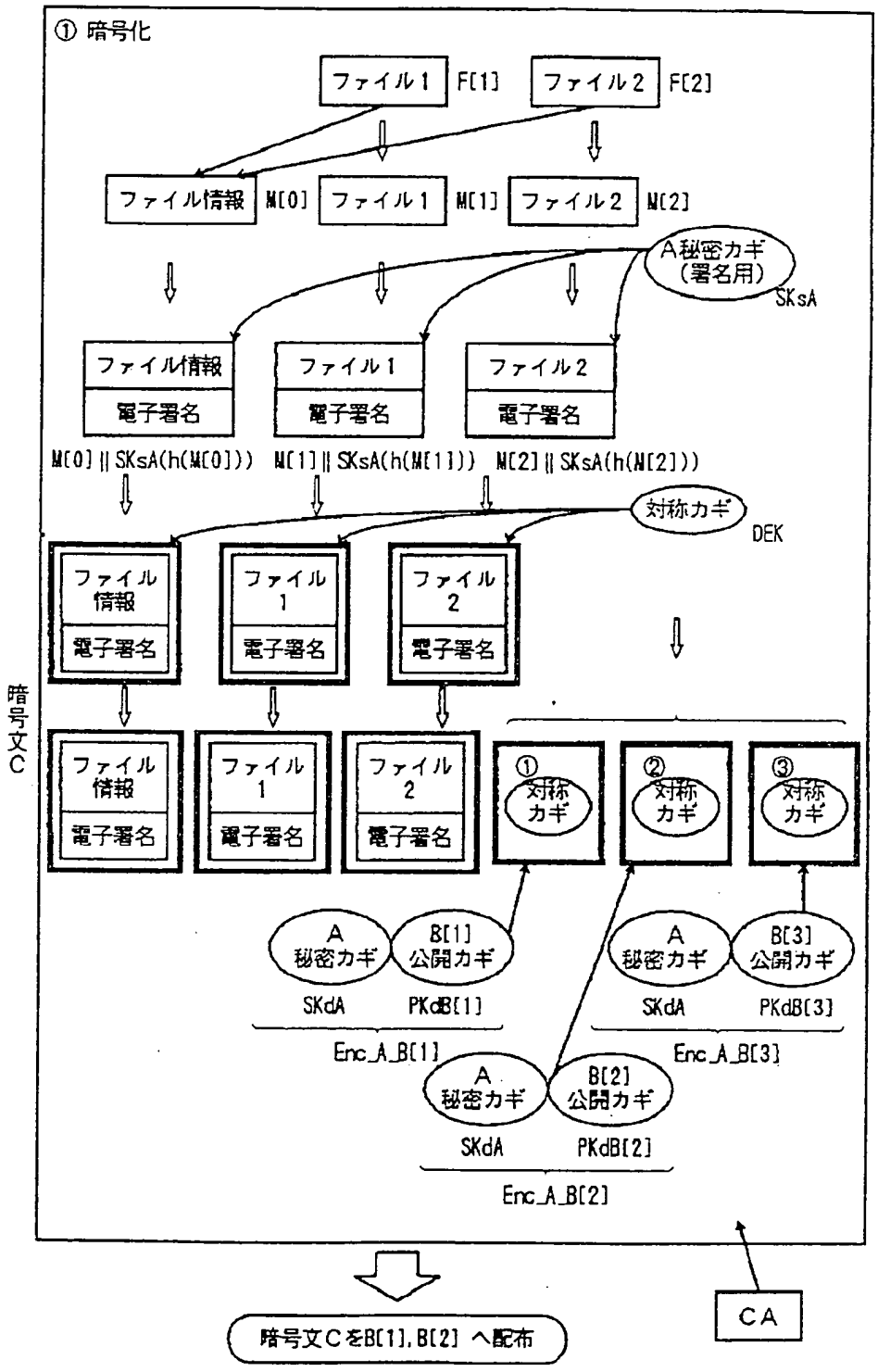

暗号化装置A
復号化装置B［i］
（i＝1，…，n）
グループ暗号化を行う前
Step4
PKdB[i](i=1,…,n) を要求
必要に応じて公開鍵を要求し、取得する
Step6
PKdB[i](i=1,…,n)
Step7　複数人暗号化
暗号文を配布
Step8
暗号文Cを配布
Enc_A_B[1](DEK)‖ …‖Enc_A_B[n](DEK)‖
DEK(M[0]‖SKsA(n(M[0])))‖…‖DEK(M[t]‖SKsA(h(M[t])))
B[i]が暗号文Cを取得・復号化する前
Step9
PKdA, PKsAを要求
必要に応じて公開鍵を要求し、取得する
Step11
PKdA, PKsA
Step12　複数人復号化

【図3】

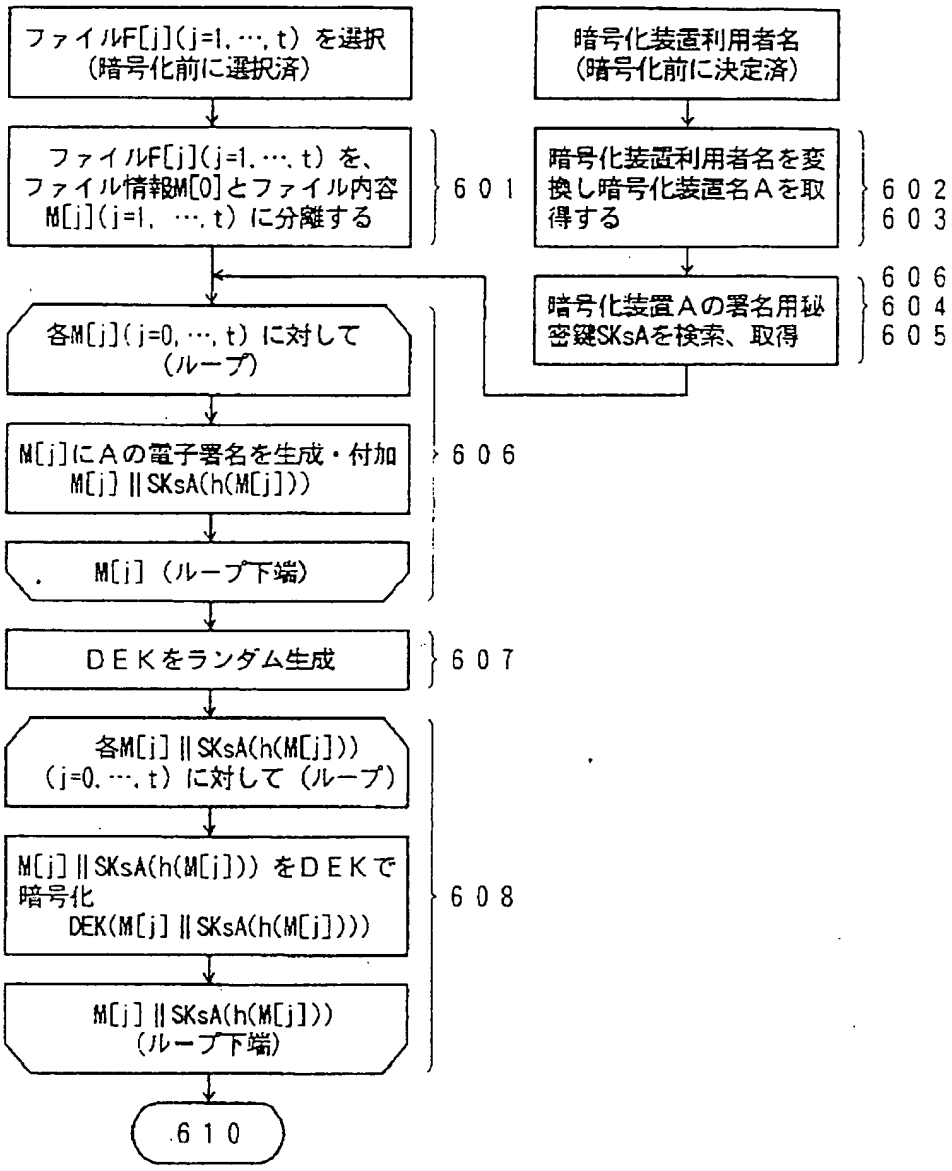
【図4】


入力
ファイルF[j]
(j=1, …, t)
暗号化装置
利用者名A
復号化装置利用
グループ名G
ファイル情報分離器 601
M[0]
M[j](j=1, …, t)
グループ情報変換器 602
グループ情報
DB 603
鍵DB
605
A及びB[i]
(i=1, …, n)
鍵検索器 604
↑要求元
↓暗号化鍵
Enc_A_B[i]
(i=1, …, n)
←Aの署名用
秘密鍵SKsA
要求元→
電子署名生成・連結器 606
M[j] || SKsA(h(M[j]))
(j=0, …, t)
暗号器 608
DEK
乱数発生器
607
DEK(M[j] || SKsA(h(M[j])))
(j=0, …, t)
複数人暗号器
609
Enc_A_B[i](DEK)
(i=1, …, n)
暗号データ連結器 610
出力
暗号文C
Enc_A_B[1](DEK) || … || Enc_A_B[n](DEK) ||
DEK(M[0] || SKsA(h(M[0]))) || … || DEK(M[t] || SKsA(h(M[t])))

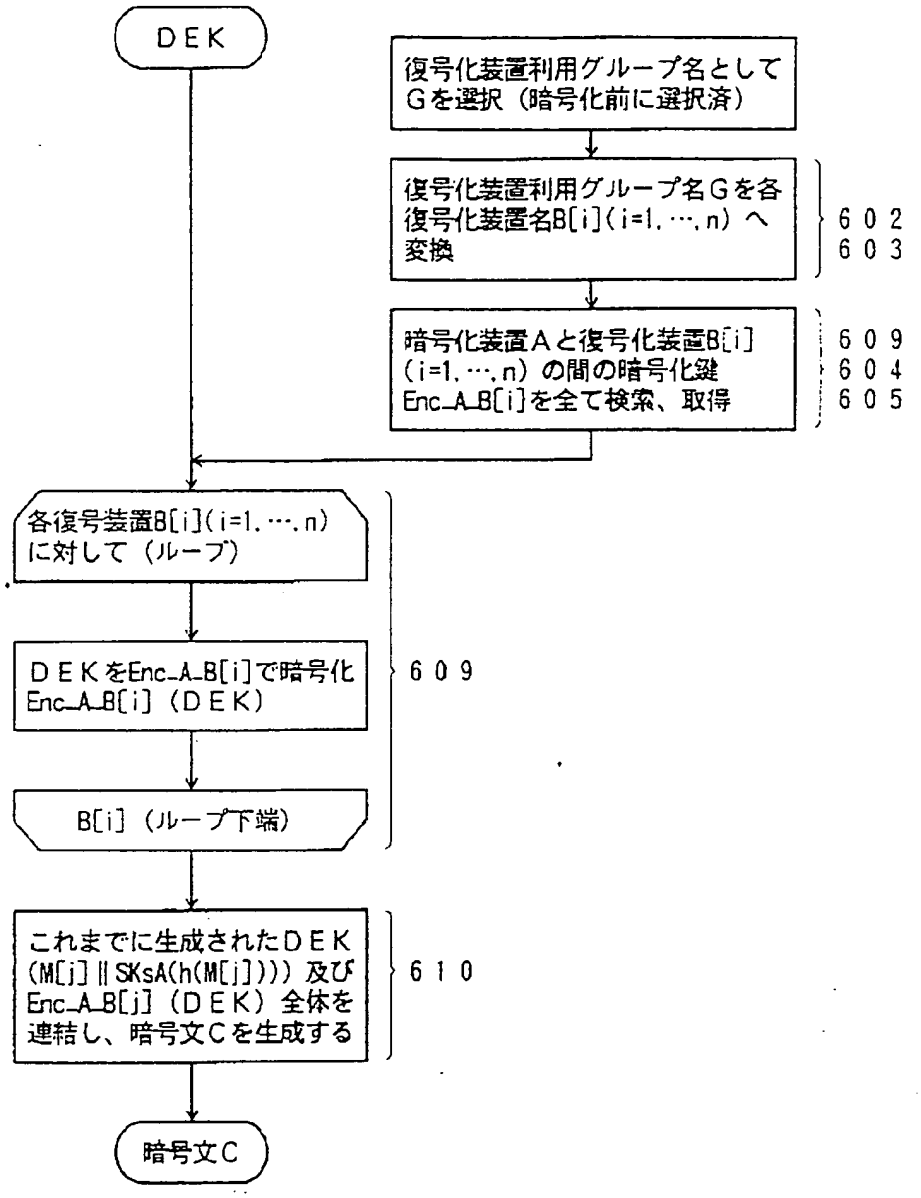
【図５】


① 暗号化
ファイル１ F[1]
ファイル２ F[2]
ファイル情報 M[0]
ファイル１ M[1]
ファイル２ M[2]
A秘密カギ（署名用） SKsA
ファイル情報 電子署名
ファイル１ 電子署名
ファイル２ 電子署名
M[0]||SKsA(h(M[0]))
M[1]||SKsA(h(M[1]))
M[2]||SKsA(h(M[2]))
対称カギ DEK
ファイル情報 電子署名
ファイル１ 電子署名
ファイル２ 電子署名
暗号文C
ファイル情報 電子署名
ファイル１ 電子署名
ファイル２ 電子署名
① 対称カギ
② 対称カギ
③ 対称カギ
A 秘密カギ SKdA
B[1] 公開カギ PKdB[1]
Enc_A_B[1]
A 秘密カギ SKdA
B[3] 公開カギ PKdB[3]
Enc_A_B[3]
A 秘密カギ SKdA
B[2] 公開カギ PKdB[2]
Enc_A_B[2]
暗号文CをB[1],B[2] へ配布
CA

【図６】

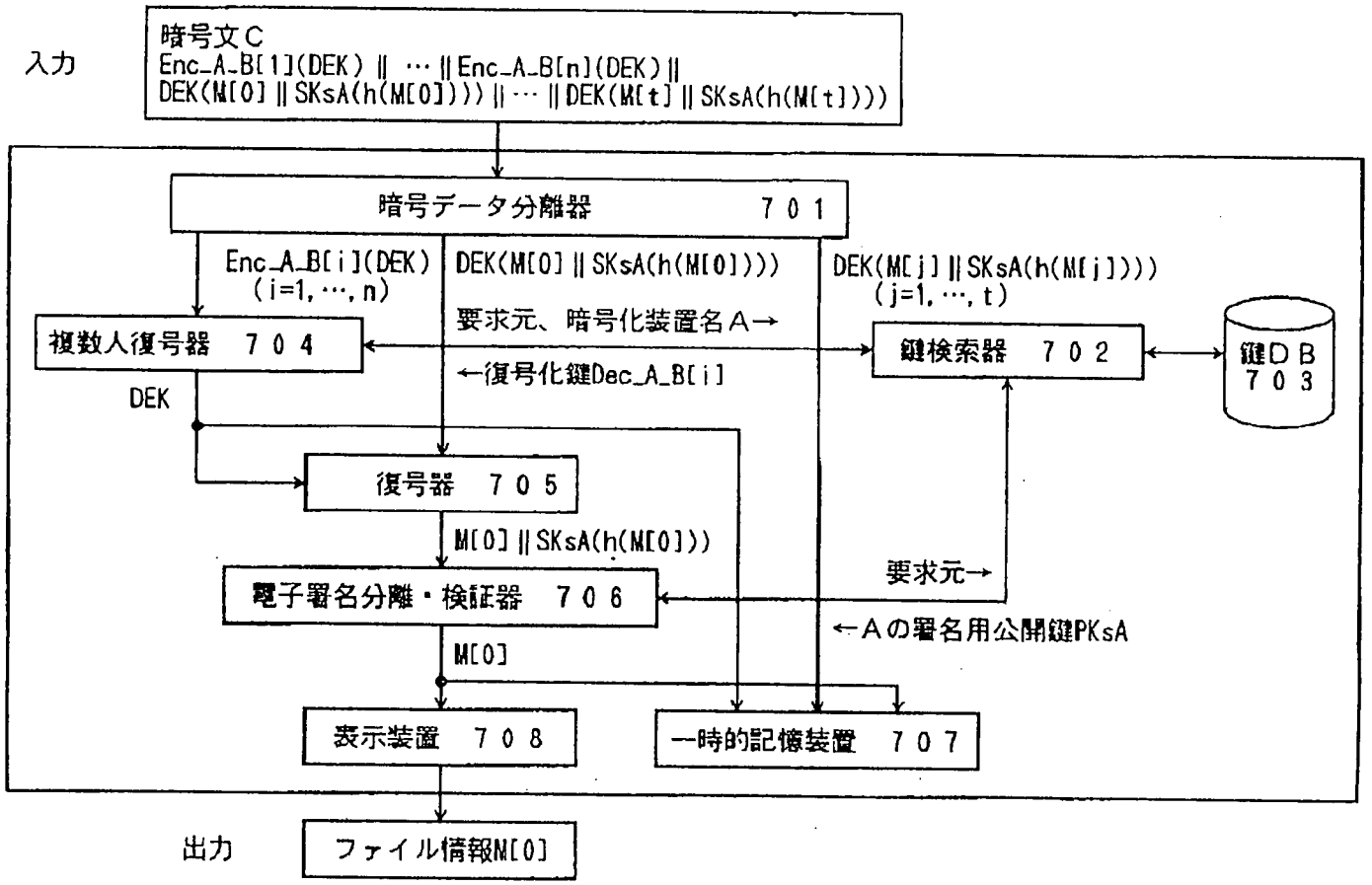

ファイルF[j](j=1, …, t) を選択
(暗号化前に選択済)
暗号化装置利用者名
(暗号化前に決定済)
ファイルF[j](j=1, …, t) を、ファイル情報M[0]とファイル内容M[j](j=1, …, t) に分離する
601
暗号化装置利用者名を変換し暗号化装置名Aを取得する
602
603
暗号化装置Aの署名用秘密鍵SKsAを検索、取得
606
604
605
各M[j](j=0, …, t) に対して(ループ)
M[j]にAの電子署名を生成・付加
M[j] || SKsA(h(M[j]))
M[j] (ループ下端)
606
DEKをランダム生成
607
各M[j] || SKsA(h(M[j]))
(j=0, …, t) に対して (ループ)
M[j] || SKsA(h(M[j])) をDEKで暗号化
DEK(M[j] || SKsA(h(M[j])))
M[j] || SKsA(h(M[j]))
(ループ下端)
608
610

【図7】

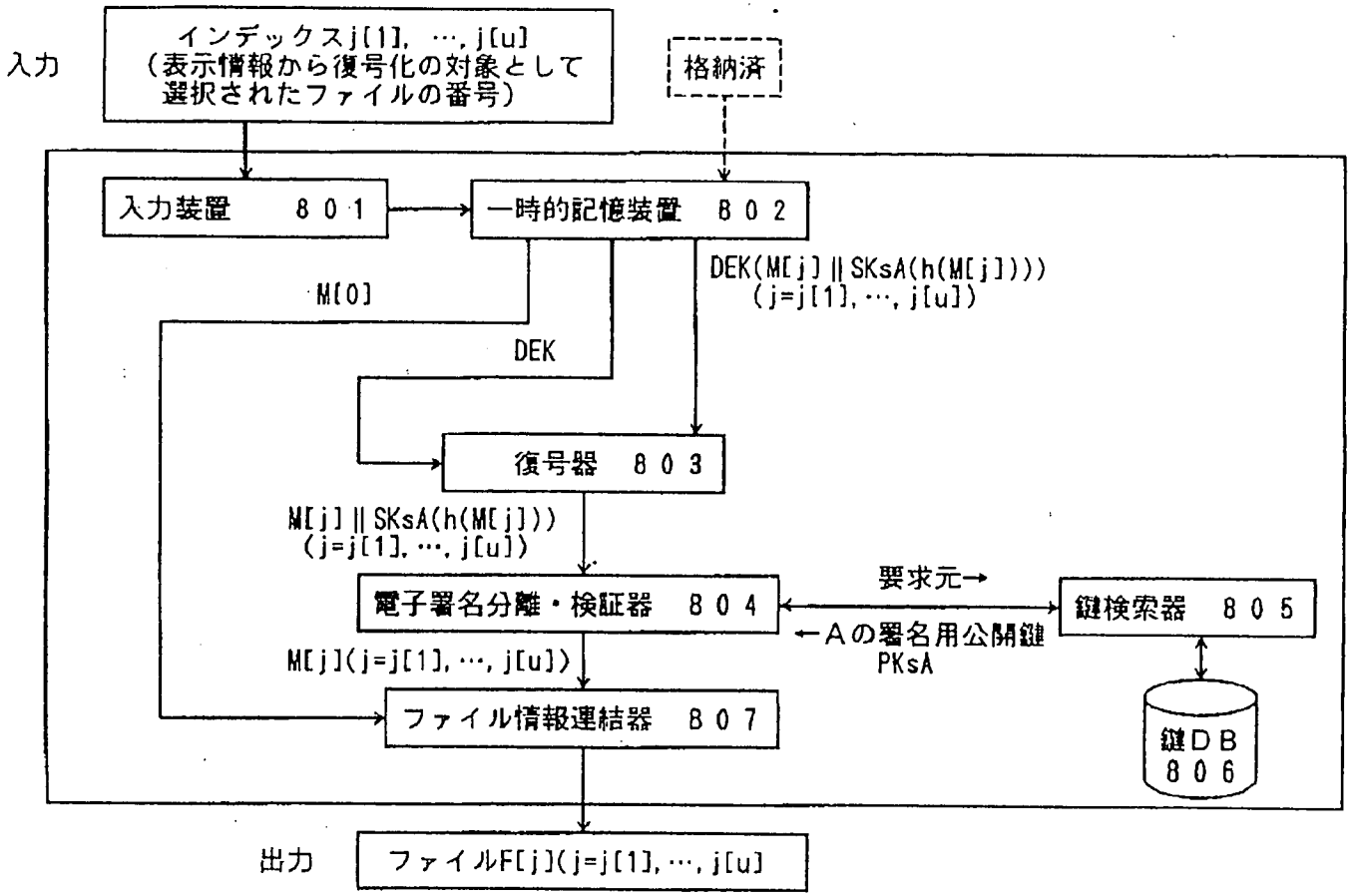


暗号文Ｃの内容

Enc_A_B[1](DEK)‖…‖Enc_A_B[n](DEK)‖
DEK(M[0]‖SKsA(h(M[0])))‖…‖DEK(M[t]‖SKsA(h(M[t])))

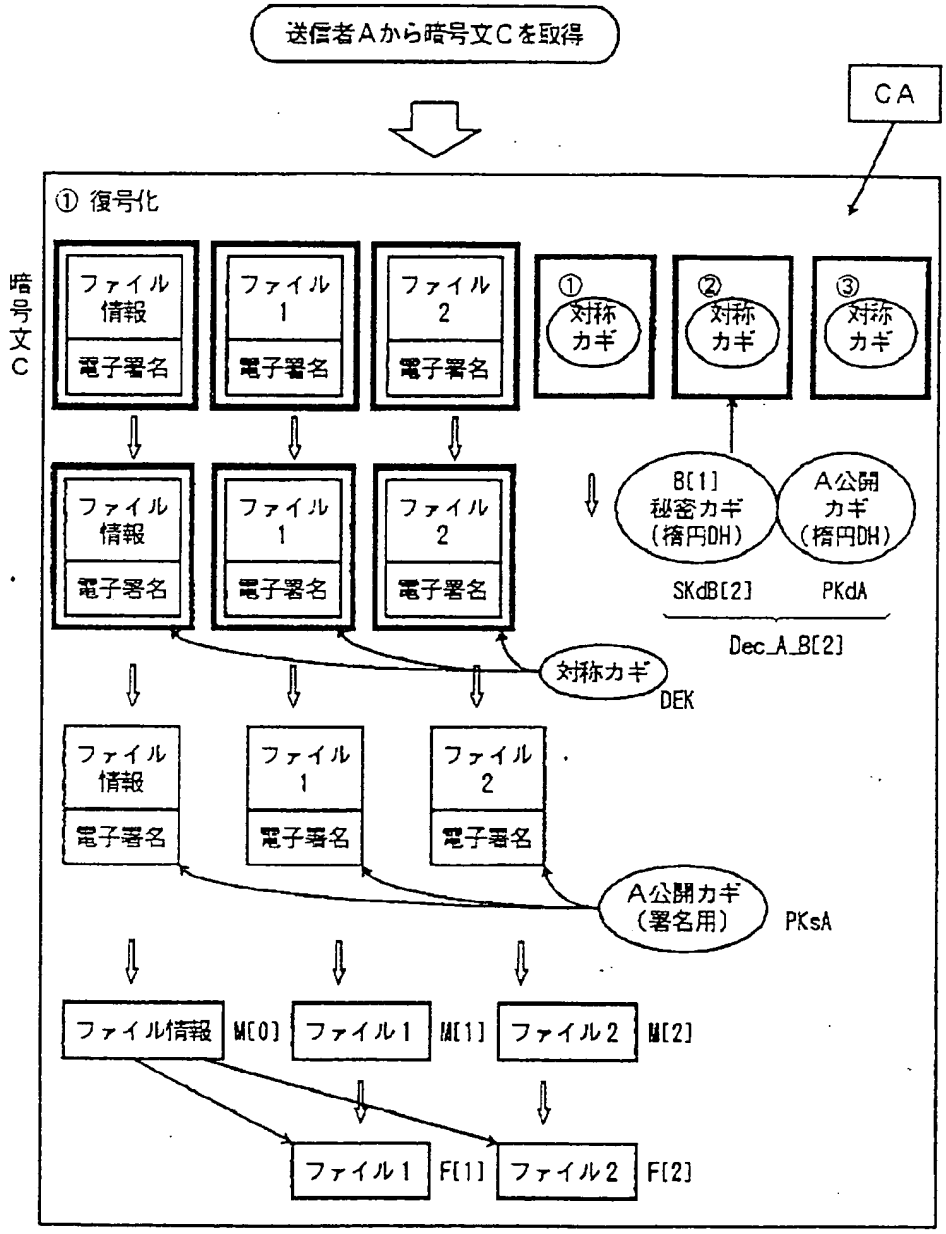

入力
暗号文C
Enc_A_B[1](DEK) ‖ … ‖Enc_A_B[n](DEK) ‖
DEK(M[0] ‖ SKsA(h(M[0]))) ‖ … ‖ DEK(M[t] ‖ SKsA(h(M[t])))
暗号データ分離器 701
Enc_A_B[i](DEK)
(i=1, …, n)
DEK(M[0] ‖ SKsA(h(M[0])))
DEK(M[j] ‖ SKsA(h(M[j])))
(j=1, …, t)
要求元、暗号化装置名A→
←復号化鍵Dec_A_B[i]
複数人復号器 704
鍵検索器 702
鍵DB 703
DEK
復号器 705
M[0] ‖ SKsA(h(M[0]))
要求元→
電子署名分離・検証器 706
←Aの署名用公開鍵PKsA
M[0]
表示装置 708
一時的記憶装置 707
出力
ファイル情報M[0]

【図8】

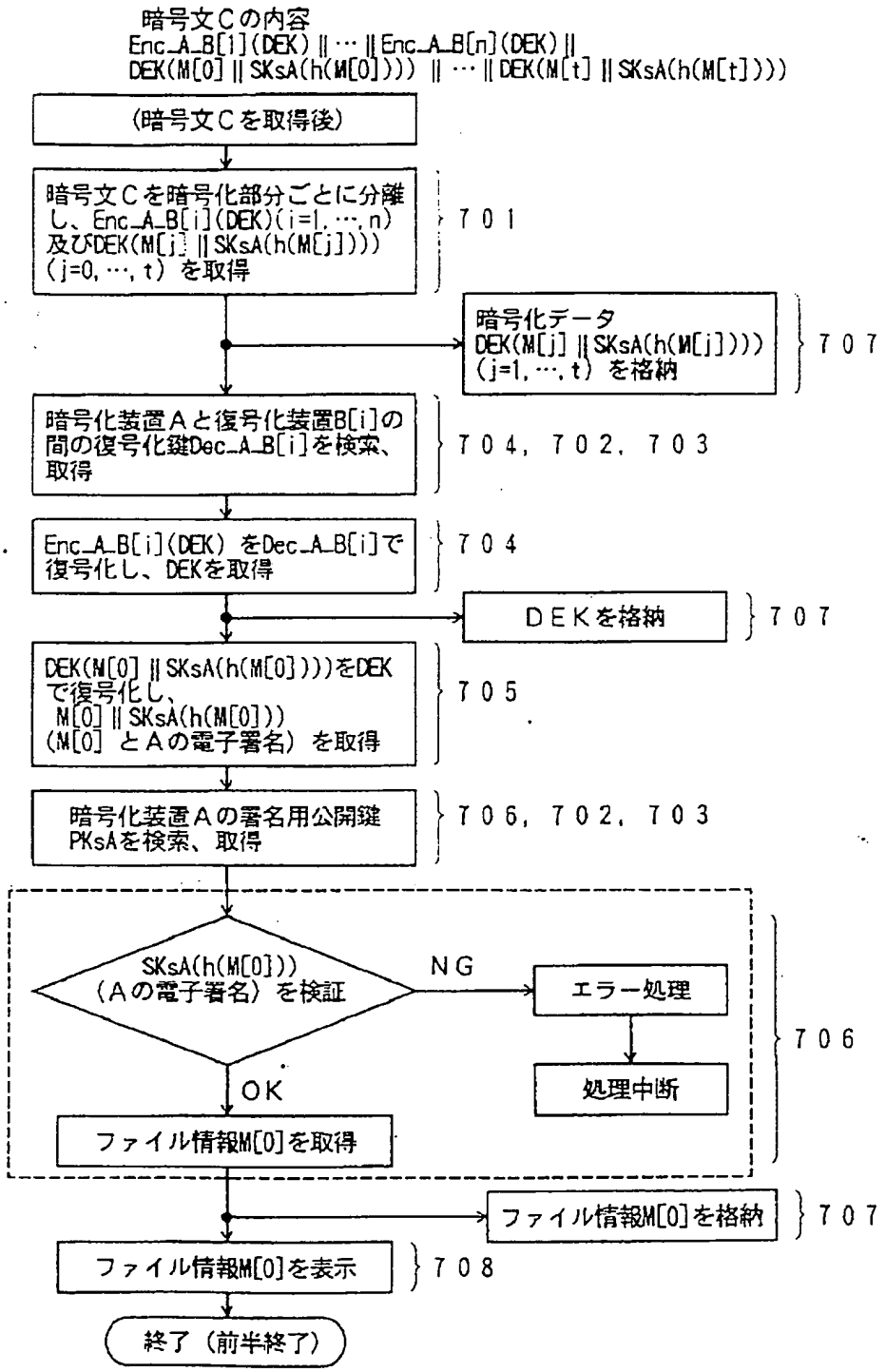

入力
インデックスj[1], …, j[u]
(表示情報から復号化の対象として
選択されたファイルの番号)
格納済
入力装置　801
一時的記憶装置　802
DEK(M[j]||SKsA(h(M[j])))
(j=j[1], …, j[u])
M[0]
DEK
復号器　803
M[j]||SKsA(h(M[j]))
(j=j[1], …, j[u])
要求元→
電子署名分離・検証器　804
←Aの署名用公開鍵
PKsA
鍵検索器　805
M[j](j=j[1], …, j[u])
ファイル情報連結器　807
鍵DB
806
出力
ファイルF[j](j=j[1], …, j[u]

[図9]

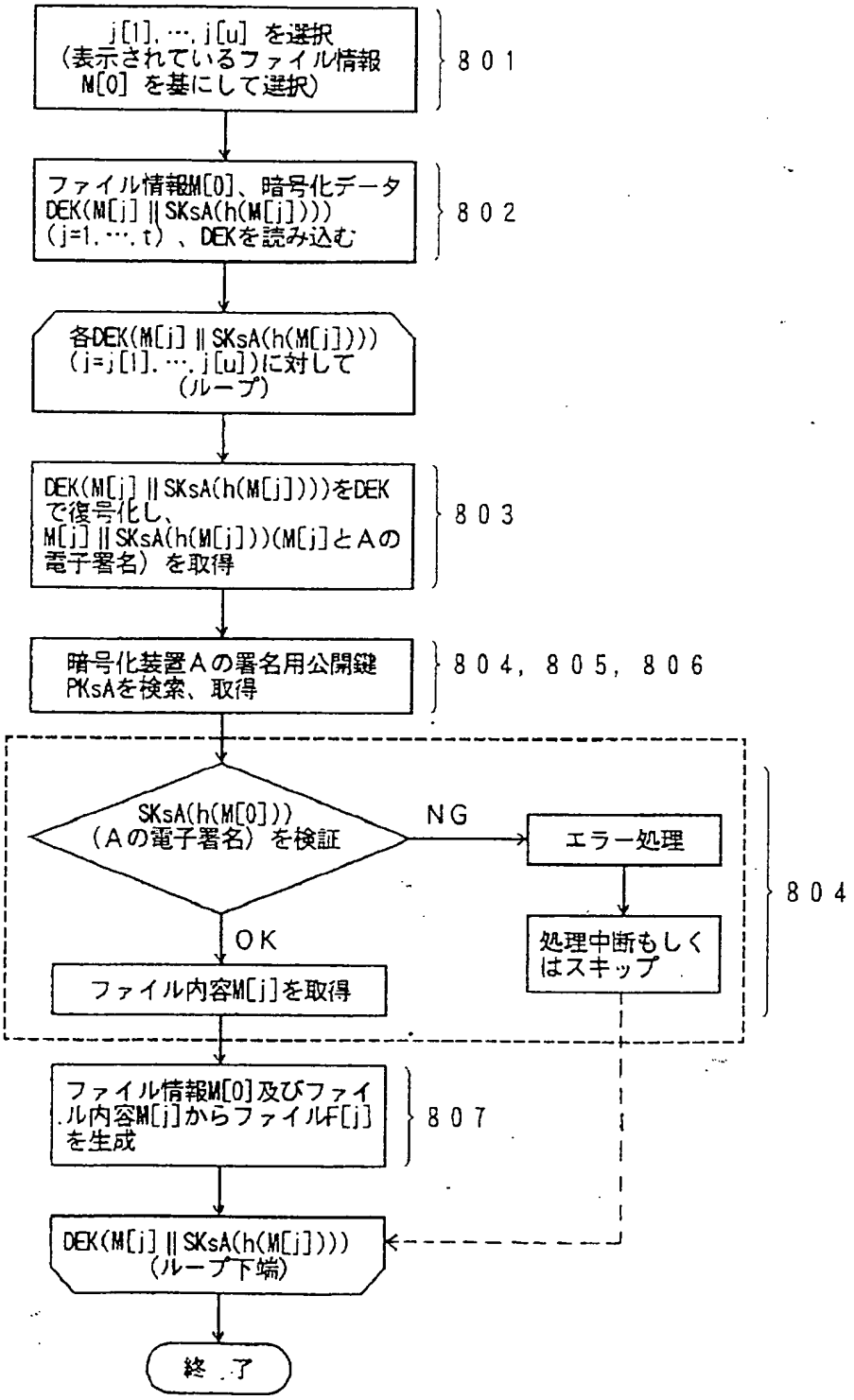
【図１０】


送信者Aから暗号文Cを取得
CA
① 復号化
暗号文C
ファイル情報
電子署名
ファイル1
電子署名
ファイル2
電子署名
①対称カギ
②対称カギ
③対称カギ
B[1]秘密カギ(楕円DH)
A公開カギ(楕円DH)
SKdB[2]
PKdA
Dec_A_B[2]
対称カギ
DEK
A公開カギ(署名用)
PKsA
ファイル情報 M[0]
ファイル1 M[1]
ファイル2 M[2]
ファイル1 F[1]
ファイル2 F[2]

【図１１】


暗号文Ｃの内容
Enc_A_B[i](DEK) ‖ … ‖Enc_A_B[n](DEK) ‖
DEK(M[0] ‖ SKsA(h(M[0]))) ‖ … ‖ DEK(M[t] ‖ SKsA(h(M[t])))
(暗号文Ｃを取得後)
暗号文Ｃを暗号化部分ごとに分離し、Enc_A_B[i](DEK)(i=1, …, n)及びDEK(M[j] ‖ SKsA(h(M[j])))(j=0, …, t) を取得
７０１
暗号化データ DEK(M[j] ‖ SKsA(h(M[j]))) (j=1, …, t) を格納
７０７
暗号化装置Ａと復号化装置B[i]の間の復号化鍵Dec_A_B[i]を検索、取得
７０４，７０２，７０３
Enc_A_B[i](DEK) をDec_A_B[i]で復号化し、DEKを取得
７０４
ＤＥＫを格納
７０７
DEK(M[0] ‖ SKsA(h(M[0])))をDEKで復号化し、M[0] ‖ SKsA(h(M[0]))(M[0] とＡの電子署名) を取得
７０５
暗号化装置Ａの署名用公開鍵PKsAを検索、取得
７０６，７０２，７０３
SKsA(h(M[0]))(Ａの電子署名) を検証
NG
エラー処理
処理中断
OK
ファイル情報M[0]を取得
７０６
ファイル情報M[0]を格納
７０７
ファイル情報M[0]を表示
７０８
終了（前半終了）

【図１２】


j[1], …, j[u] を選択
(表示されているファイル情報 M[0] を基にして選択)
801
ファイル情報M[0]、暗号化データ DEK(M[j] ‖ SKsA(h(M[j])))
(j=1, …, t) 、DEKを読み込む
802
各DEK(M[j] ‖ SKsA(h(M[j])))
(j=j[1], …, j[u])に対して
(ループ)
DEK(M[j] ‖ SKsA(h(M[j])))をDEKで復号化し、
M[j] ‖ SKsA(h(M[j]))(M[j]とAの電子署名) を取得
803
暗号化装置Aの署名用公開鍵 PKsAを検索、取得
804, 805, 806
SKsA(h(M[0]))
(Aの電子署名) を検証
NG
エラー処理
処理中断もしくはスキップ
OK
ファイル内容M[j]を取得
804
ファイル情報M[0]及びファイル内容M[j]からファイルF[j]を生成
807
DEK(M[j] ‖ SKsA(h(M[j])))
(ループ下端)
終了